

CONTENTS DATA EVALUATING DEVICE

Publication number: JP2001036856

Publication date: 2001-02-09

Inventor: TOYOKAWA KAZUHARU; MORIMOTO NORISHIGE;
TONEGAWA SATOKO

Applicant: IBM

Classification:



- international: *H04N5/91; G06F7/04; G06K9/00; H04L9/32;
H04N1/387; H04N7/167; H04N5/91; G06F7/02;
G06K9/00; H04L9/32; H04N1/387; H04N7/167; (IPC1-
7): H04N5/91; H04N1/387*

- European:

Application number: JP19990176094 19990622

Priority number(s): JP19990176094 19990622

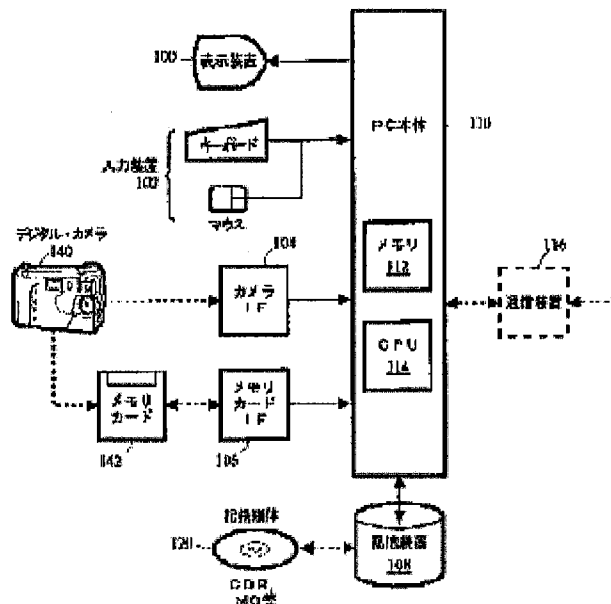
Also published as:

 US6829367 (B1)
 CA2307534 (A1)

Report a data error here

Abstract of JP2001036856

PROBLEM TO BE SOLVED: To accurately judge which part of contents data are altered since the time of preparing them by providing a means for sampling data for specifying contents and a means for judging the presence/absence of the alteration of the contents data based on this sampling result. **SOLUTION:** A picture alteration judging device compress-encodes a picture photographed by a digital camera 140 by a JPEG system, e.g. to accept via a camera IF 104. Otherwise, the device accepts compressed picture data recorded in a memory card 142 by the camera 140 through a memory card IF 106. At the time of accepting the compressed picture data, an electronic watermark (embedded data) is embedded to the compressed picture data. Then, through the use of using the character of JPEG data obtained by embedding the embedded data, a sampling part judges and displays whether the JPEG data are altered or not and when it is altered, the part decides and displays which part of the picture data are altered.



Data supplied from the esp@cenet database - Worldwide

Family list4 family members for: **JP2001036856**

Derived from 3 applications

[Back to JP2001036856](#)**1 CONTENT DATA JUDGING APPARATUS****Inventor:** TONEGAWA SATOKO (JP); MORIMOTO NORISHIGE (JP); (+1) **Applicant:** IBM (US)**EC:** **IPC:** H04N5/91; G06F7/04; G06K9/00 (+11)**Publication info:** CA2307534 A1 - 2000-12-22**2 CONTENTS DATA EVALUATING DEVICE****Inventor:** TOYOKAWA KAZUHARU; MORIMOTO NORISHIGE; (+1) **Applicant:** IBM**EC:** **IPC:** H04N5/91; G06F7/04; G06K9/00 (+11)**Publication info:** JP3342677B2 B2 - 2002-11-11**JP2001036856 A** - 2001-02-09**3 Content data judging apparatus****Inventor:** TOYOKAWA KAZUHARA (JP); MORIMOTO NORISHIGE (JP); (+1) **Applicant:** IBM (US)**EC:** **IPC:** H04N5/91; G06F7/04; G06K9/00 (+11)**Publication info:** US6829367 B1 - 2004-12-07

Data supplied from the esp@cenet database - Worldwide

(11)特許出願公開番号

特開2001-36856

(P2001-36856A)

(43)公開日 平成13年2月9日(2001.2.9)

(51) Int.Cl.⁷

識別記号

FI

テーマト* (参考)

H0 4 N 5/91

H04N 5/91

P 5C053

1/387

1/387

5 C 0 7 6

審査請求 有 請求項の数15 O.L (全 36 頁)

(21)出願番号

特願平11-176094

(22) 出題日

平成11年6月22日(1999.6.22)

(71)出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション

INTERNATIONAL BUSIN
ESS MASCHINES CORPO
RATION

アメリカ合衆国10504、ニューヨーク州

アーモンク (番地なし)

(74) 代理人 100086243

弁理士 坂口 博 (外1名)

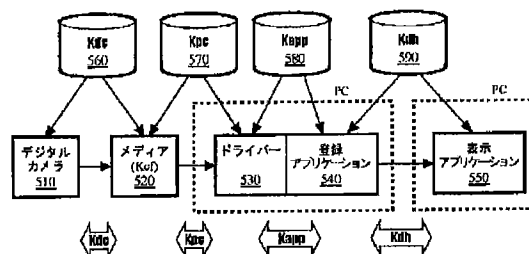
[最終頁に続く](#)

(54) 【発明の名称】 コンテンツデータ鑑定装置

(57) 【要約】 (修正有)

【課題】 コンテンツデータ作成時点からどこが改変されたかを正確に判定する鑑定方法を提供する。

【解決手段】（１）コンテンツデータを記録したメディアと認証を行う手段と、（２）メディアに記録されたコンテンツデータを読み取る手段と、（３）コンテンツデータに、該コンテンツを特定するデータを埋め込む手段と、（４）コンテンツを特定するデータの埋め込まれたコンテンツデータから、該コンテンツを特定するデータを抽出する手段と、（５）コンテンツを特定するデータの抽出結果に基づき、コンテンツデータ改変の有無の判断を行う手段と、コンテンツデータに改変がなされたと判断した場合に、改変個所の特定を行う手段を有する。



【特許請求の範囲】

【請求項1】デジタルデバイスで作成されたコンテンツデータに改変がなされたかどうかを鑑定する、コンテンツデータ鑑定装置であって、(1)コンテンツデータを記録したメディアと認証を行う手段と、(2)前記メディアに記録されたコンテンツデータを読み取る手段と、(3)前記コンテンツデータに、該コンテンツを特定するデータを埋め込む手段と、(4)前記コンテンツを特定するデータの埋め込まれたコンテンツデータから、該コンテンツを特定するデータを抽出する手段と、(5)前記コンテンツを特定するデータの抽出結果に基づき、コンテンツデータ改変の有無の判断を行う手段とを有する、コンテンツデータ鑑定装置。

【請求項2】前記コンテンツデータ改変の有無の判断を行う手段(5)が、コンテンツデータに改変がなされたと判断した場合に、改変個所の特定を行う手段を有する、請求項1記載の装置。

【請求項3】前記コンテンツデータを読み取る手段(2)において、前記メディアに記録されたコンテンツデータが、デジタルデバイスと前記メディアとの認証結果を含み、該認証結果を読み取る手段を有する、請求項1記載の装置。

【請求項4】前記コンテンツを特定するデータ埋め込む手段(3)が、コンテンツデータに、コンテンツデータの認証履歴情報、作成日、作成者、作成機器、登録日などを含むID情報を埋め込む手段を有する、請求項1記載の装置。

【請求項5】デジタルデバイスで作成されたコンテンツデータに、改変検出用データを埋め込む装置であって、(1)コンテンツデータを記録したメディアと認証を行う手段と、(2)前記メディアに保存されたコンテンツデータを読み取る手段と、(3)前記コンテンツデータに、改変個所の特定を行う改変検出用データを埋め込み、記憶する手段と、を有する、改変検出用データ埋め込み装置。

【請求項6】コンテンツデータ改変鑑定装置であって、(1)改変検出用データの埋め込まれたコンテンツデータから、改変検出用データを抽出する手段と、(2)前記改変検出用データの抽出結果に基づき、コンテンツデータ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う手段と、を有する、コンテンツデータ改変鑑定装置。

【請求項7】前記デジタルデバイスが、カメラ、録音装置、スキャナ、もしくはビデオカメラである、請求項1～請求項5の何れかに記載の装置。

【請求項8】デジタルカメラと、デジタルカメラで作成された画像を記録する記録メディアと、記録メディアにアクセスし画像データを読み取り電子透かしを埋め込む電子透かし埋め込み装置と、画像データに埋め込まれた電子透かしを抽出する電子透かし抽出装置、からなる画

像データ鑑定装置であって、(1)デジタルカメラで画像データを作成する手段と、(2)デジタルカメラと画像記録メディア間で認証を行う手段と、(3)前記認証が成功した場合、前記画像データを前記画像記録メディアに記録する手段と、(4)前記記録メディアと電子透かし埋め込み装置間で認証を行う手段と、(5)前記認証が成功した場合、前記電子透かし埋め込み装置が、前記記録メディアから前記画像データを読み取る手段と、

(6)前記電子透かし埋め込み装置が、前記画像データに、改変判定のためのデータを、複数の前記認証の結果および画像データに関連するID情報と共に、電子透かしとして埋め込む手段と、(7)前記電子透かし埋め込み装置が、前記電子透かしの埋め込まれた、前記画像データを記憶装置に記録する手段と、(8)電子透かし検出装置が、前記記憶装置に記録された画像データを読み取り、該画像データに埋め込まれた電子透かしを抽出する手段と、(9)前記電子透かし検出装置が、抽出された前記電子透かしの結果から、前記画像データに改変がなされたかどうかを判断し、改変がなされた判断した場合、改変の個所を特定する手段と、を有する、画像データ鑑定装置。

【請求項9】デジタルカメラで作成された画像を鑑定する方法であって、(1)デジタルカメラで画像データを作成する段階と、(2)デジタルカメラと画像記録メディア間で認証を行う段階と、(3)前記認証が成功した場合、前記画像データを前記画像記録メディアに記録する段階と、(4)前記記録メディアとデバイスドライバ間で認証を行う段階と、(5)前記認証が成功した場合、前記デバイスドライバと、電子透かしを埋め込む電子透かし埋め込みプログラム間で認証を行う段階と、

(6)前記電子透かし埋め込みプログラムが、前記記録メディアから前記画像データを読み取る段階と、(7)前記電子透かし埋め込みプログラムが、前記画像データに、改変判定のためのデータを、複数の前記認証の結果および画像データに関連するID情報と共に、電子透かしとして埋め込む段階と、(8)前記電子透かし埋め込みプログラムが、前記電子透かしの埋め込まれた、前記画像データを記憶装置に記録する段階と、(9)電子透かし検出プログラムが、前記記憶装置に記録された画像データを読み取り、該画像データに埋め込まれた電子透かしを抽出する段階と、(10)前記電子透かし検出プログラムが、抽出された前記電子透かしの結果から、前記画像データに改変がなされたかどうかを判断し、改変がなされたと判断した場合、改変の個所を特定する段階と、を有する、画像データ鑑定方法。

【請求項10】証拠データの改変やすり替えを検知することにより、損害査定業務プロセスを、安全かつ効率的に行う、保険業務処理システムであって、(1)デジタルデバイスを用いて損害対象物の証拠データを作成する手段と、(2)前記証拠データに改変検出用データを

埋め込み、記憶装置に記録する手段と、(3)前記改変検出用データの埋め込まれた証拠データから、前記改変検出用データを抽出し、該抽出の結果に基づき、証拠データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行うことにより、前記記憶装置に記録された前記証拠データを鑑定する手段と、を有する、保険業務処理システム。

【請求項11】証拠データの改変やすり替えを検知することにより、損害査定業務プロセスを、安全かつ効率的に行う、保険業務の実施方法であって、(1)デジタルデバイスを用いて損害対象物の証拠データを作成する段階と、(2)前記証拠データに改変検出用データを埋め込み、記憶装置に記録する段階と、(3)前記改変検出用データの埋め込まれた証拠データから、前記改変検出用データを抽出し、該抽出の結果に基づき、証拠データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行うことにより、前記記憶装置に記録された前記証拠データを鑑定する段階と、を有する、保険業務の実施方法。

【請求項12】所有者の証明を行うスマートカードであって、(1)所有者の名前またはカード番号が記載されたカード面と、(2)改変個所特定を行う改変検出用データが埋め込まれた所有者の証明データを記憶した記憶装置と、を有する、スマートカード。

【請求項13】スマートカードに記憶されたデータを読み取るスマートカード・リーダを有する、証明データ検出装置であって、(1)改変検出用データが埋め込まれた所有者の証明データをスマートカードから読み取る手段と、(2)前記改変検出用データの抽出結果に基づき、前記証明データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う手段、を有する、証明データ検出装置。

【請求項14】デジタルデバイスで作成されたコンテンツデータを記憶装置に記録するプログラムを含む、媒体であって、(1)コンテンツデータを記録した記録メディアと認証を行う機能と、(2)前記記録メディアに記録されたコンテンツデータを読み取る機能と、(3)前記コンテンツデータに、改変個所の特定を行う改変検出用データを埋め込み、記憶装置に記録する機能と、をコンピュータに実行させるプログラムを含む媒体。

【請求項15】記録されたコンテンツデータの改変を鑑定するプログラムを含む媒体であって、(1)改変検出用データの埋め込まれたコンテンツデータから、改変検出用データを抽出する機能と、(2)前記改変検出用データの抽出結果に基づき、コンテンツデータ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う機能と、をコンピュータに実行させるプログラムを含む媒体。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、デジタルデバイスにより作成された画像、音声などのコンテンツデータに電子透かしを埋め込み、埋め込んだ電子透かしを検出することによりコンテンツデータの鑑定を行う装置およびその方法に関し、特にコンテンツデータを証拠物件として扱えるように、デジタルデバイス、記録メディア、複数のプログラム間で、認証を適切に行うことによりセキュリティを高度に保持し、コンテンツデータになされた改変の有無及び改変個所の特定を行うことのできる、コンテンツデータ鑑定装置および方法、該装置および方法を用いた保険業務処理システムに関する発明である。

【0002】

【従来の技術】従来、画像データの改変を検出する方法としてハッシュ関数を用いる方法が知られている。この方法はあらかじめハッシュ関数等を用いて作成された情報を画像データに付加し、改変判定時に、この情報と、画像データに基づき作成したハッシュ値を比較することにより改変が加えられているか否か判断する方法である。しかしながらこのような方式は、画像データに改変がなされたかどうかを検出することはできても、具体的に、画像データのいずれの部分に改変が加えられているかを判定して示すことはできない。これを克服する発明として、特願平11-158358がある。この発明は改変検出のための付加情報をコンテンツデータに電子透かしで埋め込み、この付加情報を検出することによりコンテンツデータになされた改変の位置を特定する方法が記載されている。

【0003】しかしながら、この方法はコンテンツデータの鑑定のしくみを提供しない。ここで鑑定とは、コンテンツデータ作成時点から、コンテンツデータの改変判定時点までにおいて確実にコンテンツデータが受け渡されてきたか、改変がなされている場合、どの過程において改変された可能性があるか、どこが改変されたかを正確に判定する作業を指す。

【0004】さらに、従来の方法は、カメラ、録音装置、スキャナ、ビデオカメラなどのデジタルデバイスにより作成されたコンテンツデータを証拠物件として扱えるようにするための、高度なセキュリティ保持のしくみ、あるいはこれらのコンテンツデータを用いたクレームサービスおよび保険業務処理を行うプロセスを提供しない。

【0005】さらに、従来の方法は、本人証明を行う証明物に改ざんがあるかないかを判断し、その改ざんの個所を特定するための機構を提供しない。

【0006】さらに、従来の方法は、コンテンツデータを作成するデジタルデバイスの種類に関係しない、統一したコンテンツデータの鑑定方法および鑑定装置を提供しない。

【0007】

【発明が解決しようとする課題】本発明は、上述した従

来技術の問題点に鑑みてなされたものであり、コンテンツデータ作成時点から、コンテンツデータの改変判定時点までにおいて確実にコンテンツデータが受け渡されてきたか、改変がなされている場合、どの過程において改変された可能性があるか、どこが改変されたかを正確に判定する、コンテンツデータ鑑定装置およびその方法を提供することを目的とする。

【0008】また別の課題は、コンテンツデータが確実に受け渡されてきたかを証明する、高度なセキュリティ保持のしくみや、そのしくみをういたクレームサービスおよび保険業務処理を行う方法およびそのシステムを提供することである。

【0009】また別の課題は、本人証明のための、証明物に改ざんがあるかないかを判断し、その改ざんの個所を特定するための方法およびシステムを提供することである。

【0010】

【課題を達成するための手段】[コンテンツデータ鑑定装置] デジタルデバイスで作成されたコンテンツデータに改変がなされたかどうかを鑑定する、コンテンツデータ鑑定装置は、(1) コンテンツデータを記録したメディアと認証を行う手段と、(2) 前記メディアに記録されたコンテンツデータを読み取る手段と、(3) 前記コンテンツデータに、該コンテンツを特定するデータを埋め込む手段と、(4) 前記コンテンツを特定するデータの埋め込まれたコンテンツデータから、該コンテンツを特定するデータを抽出する手段と、(5) 前記コンテンツを特定するデータの抽出結果に基づき、コンテンツデータ改変の有無の判断を行う手段とを有する。好適には、前記コンテンツデータ改変の有無の判断を行う手段(5)が、コンテンツデータに改変がなされたと判断した場合に、改変個所の特定を行う手段を有する。

【0011】好適には、前記コンテンツデータを読み取る手段(2)において、前記メディアに記録されたコンテンツデータが、デジタルデバイスと前記メディアとの認証結果を含み、該認証結果を読み取る手段を有する。

【0012】好適には、前記コンテンツを特定するデータ埋め込む手段(3)が、コンテンツデータに、コンテンツデータの認証履歴情報、作成日、作成者、作成機器、登録日などを含むID情報を埋め込む手段を有する。

【0013】[改変検出用データ埋め込み装置] デジタルデバイスで作成されたコンテンツデータに、改変検出用データを埋め込む装置は、(1) コンテンツデータを記録したメディアと認証を行う手段と、(2) 前記メディアに保存されたコンテンツデータを読み取る手段と、(3) 前記コンテンツデータに、改変個所の特定を行う改変検出用データを埋め込み、記憶する手段とを有する。

【0014】[コンテンツデータ改変鑑定装置] コンテ

ンツデータ改変鑑定装置は、(1) 改変検出用データの埋め込まれたコンテンツデータから、改変検出用データを抽出する手段と、(2) 前記改変検出用データの抽出結果に基づき、コンテンツデータ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う手段とを有する。

【0015】[画像データ鑑定装置] デジタルカメラと、デジタルカメラで作成された画像を記録する記録メディアと、記録メディアにアクセスし画像データを読み取り電子透かしを埋め込む電子透かし埋め込み装置と、画像データに埋め込まれた電子透かしを抽出する電子透かし抽出装置、からなる画像データ鑑定装置は、(1) デジタルカメラで画像データを作成する手段と、(2) デジタルカメラと画像記録メディア間で認証を行う手段と、(3) 前記認証が成功した場合、前記画像データを前記画像記録メディアに記録する手段と、(4) 前記記録メディアと電子透かし埋め込み装置間で認証を行う手段と、(5) 前記認証が成功した場合、前記電子透かし埋め込み装置が、前記記録メディアから前記画像データを読み取る手段と、(6) 前記電子透かし埋め込み装置が、前記画像データに、改変判定のためのデータを、複数の前記認証の結果および画像データに関連するID情報と共に、電子透かしとして埋め込む手段と、(7) 前記電子透かし埋め込み装置が、前記電子透かしの埋め込まれた、前記画像データを記憶装置に記録する手段と、(8) 電子透かし検出装置が、前記記憶装置に記録された画像データを読み取り、該画像データに埋め込まれた電子透かしを抽出する手段と、(9) 前記電子透かし検出装置が、抽出された前記電子透かしの結果から、前記画像データに改変がなされたかどうかを判断し、改変がなされたと判断した場合、改変の個所を特定する手段と、を有する。

【0016】[画像データ鑑定方法] デジタルカメラで作成された画像を鑑定する方法は、(1) デジタルカメラで画像データを作成する段階と、(2) デジタルカメラと画像記録メディア間で認証を行う段階と、(3) 前記認証が成功した場合、前記画像データを前記画像記録メディアに記録する段階と、(4) 前記記録メディアとデバイスドライバ間で認証を行う段階と、(5) 前記認証が成功した場合、前記デバイスドライバと、電子透かしを埋め込む電子透かし埋め込みプログラム間で認証を行う段階と、(6) 前記電子透かし埋め込みプログラムが、前記記録メディアから前記画像データを読み取る段階と、(7) 前記電子透かし埋め込みプログラムが、前記画像データに、改変判定のためのデータを、複数の前記認証の結果および画像データに関連するID情報と共に、電子透かしとして埋め込む段階と、(8) 前記電子透かし埋め込みプログラムが、前記電子透かしの埋め込まれた、前記画像データを記憶装置に記録する段階と、(9) 電子透かし検出プログラムが、前記記憶装置に記

録された画像データを読み取り、該画像データに埋め込まれた電子透かしを抽出する段階と、(10)前記電子透かし検出プログラムが、抽出された前記電子透かしの結果から、前記画像データに改変がなされたかどうかを判断し、改変がなされたと判断した場合、改変の個所を特定する段階とを有する。

【0017】[保険業務処理システム]証拠データの改変やすり替えを検知することにより、損害査定の業務プロセスを、安全かつ効率的に行う、保険業務処理システムは、(1)デジタルデバイスを用いて損害対象物の証拠データを作成する手段と、(2)前記証拠データに改変検出用データを埋め込み、記憶装置に記録する手段と、(3)前記改変検出用データの埋め込まれた証拠データから、前記改変検出用データを抽出し、該抽出の結果に基づき、証拠データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行うことにより、前記記憶装置に記録された前記証拠データを鑑定する手段と、を有する。

【0018】[保険業務の実施方法]証拠データの改変やすり替えを検知することにより、損害査定の業務プロセスを、安全かつ効率的に行う、保険業務の実施方法は、(1)デジタルデバイスを用いて損害対象物の証拠データを作成する段階と、(2)前記証拠データに改変検出用データを埋め込み、記憶装置に記録する段階と、(3)前記改変検出用データの埋め込まれた証拠データから、前記改変検出用データを抽出し、該抽出の結果に基づき、証拠データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行うことにより、前記記憶装置に記録された前記証拠データを鑑定する段階とを有する。

【0019】[スマートカード]所有者の証明を行うスマートカードは、(1)所有者の名前またはカード番号が記載されたカード面と、(2)改変個所特定を行う改変検出用データが埋め込まれた所有者の証明データを記憶した記憶装置とを有する。

【0020】[証明データ検出装置]スマートカードに記憶されたデータを読み取るスマートカード・リーダーを有する、証明データ検出装置は、(1)改変検出用データが埋め込まれた所有者の証明データをスマートカードから読み取る手段と、(2)前記改変検出用データの抽出結果に基づき、前記証明データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う手段を有する。

【0021】[改変検出用データを埋め込むプログラムを含む媒体]デジタルデバイスで作成されたコンテンツデータに改変検出用データを埋め込むプログラムを含む、媒体は、(1)コンテンツデータを記録した記録メディアと認証を行う機能と、(2)前記記録メディアに記録されたコンテンツデータを読み取る機能と、(3)前記コンテンツデータに、改変個所の特定を行う改変検

出用データを埋め込み、記憶装置に記録する機能とをコンピュータに実行させるプログラムを含む。

【0022】[コンテンツデータの改変を鑑定するプログラムを含む媒体]記録されたコンテンツデータの改変を鑑定するプログラムを含む媒体は、(1)改変検出用データの埋め込まれたコンテンツデータから、改変検出用データを抽出する機能と、(2)前記改変検出用データの抽出結果に基づき、コンテンツデータ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う機能とをコンピュータに実行させるプログラムを含む。

【0023】なお、好適には上記デジタルデバイスは、カメラ、録音装置、スキャナ、もしくはビデオカメラである。またコンテンツデータに改変検出用データを埋め込む手段と、改変検出用データの埋め込まれたコンテンツデータから該改変検出用データを抽出する手段と、改変検出用データの抽出結果に基づき、コンテンツデータ改変の有無の判断、あるいは改変がなされた場合に改変個所の特定を行う手段に関しては、以下の改変判定装置に詳細に記す。

【0024】[改変判定装置]本発明にかかるコンテンツ改変判定装置は、所定の埋め込みデータを埋め込む対象となるコンテンツデータに前記埋め込みデータを付加する、改変検出用データ埋め込み手段(以降データ付加装置と記す)と、前記所定の埋め込みデータが埋め込まれたコンテンツデータに対して改変が加えられたか否かを判定する判定装置とを有する改変判定装置であって、前記データ付加装置は、前記コンテンツデータの少なくとも一部を複数の第1のブロックに分割するコンテンツデータ分割手段と、分割の結果として得られた前記複数の第1のブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、複数の第2のブロックとする埋め込みデータ付加手段とを有し、前記判定装置は、前記第2のブロックの少なくとも一部それぞれに付加された前記埋め込みデータ(第2の埋め込みデータ)を抽出する埋め込みデータ抽出手段(改変検出用データ抽出手段)と、抽出された前記第2の埋め込みデータに基づいて、前記第2のブロックの少なくとも一部それぞれに改変が加えられたか否かを判定する改変判定手段(改変個所特定手段)とを有する。

【0025】好適には、画像データに所定の埋め込みデータを付加するデータ付加装置と、前記所定の埋め込みデータが埋め込まれた画像データに対して改変が加えられたか否かを判定する判定装置とを有する改変判定装置であって、前記データ付加装置は、画像データを複数の第1の画像ブロックに分割する画像分割手段と、分割の結果として得られた前記複数の第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、複数の第2の画像ブロックとする埋め込みデータ付加手段とを有し、前記判定装置は、前記第2の画像プロ

ックそれぞれに付加された埋め込みデータ(第2の埋め込みデータ)を抽出する埋め込みデータ抽出手段と、抽出された前記第2の埋め込みデータに基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定手段とを有する。

【0026】好適には、前記画像分割手段は、前記画像データを、それぞれ複数の単位データを含む前記複数の第1の画像ブロックに分割し、前記埋め込みデータ付加手段は、互いに対応する2つ以上の前記第1の画像ブロックそれぞれに含まれ、互いに対応する複数の前記単位データの値の関係が、所定の規則に従って前記第1の埋め込みデータを表すように調整して、前記複数の第1の画像ブロックそれぞれに前記第1の埋め込みデータを付加することにより、前記第2の画像ブロックとする。

【0027】好適には、前記埋め込みデータ付加手段は、いずれかの前記第2の画像ブロックに対して改変が加えられた場合に、改変が加えられた前記第2の画像ブロックに含まれ、互いに対応する前記複数の単位データの値が、前記所定の規則に従わなくなるように調整する。

【0028】好適には、前記埋め込みデータ抽出手段は、前記複数の第2の画像ブロックそれぞれから、前記第2の画像ブロックそれぞれに含まれる前記複数の単位データの値の関係が、前記所定の規則に従って表すデータを、前記第2の埋め込みデータとして抽出する。好適には、前記改変判定手段は、埋め込まれた前記第1の埋め込みデータと、抽出された前記第2の埋め込みデータとの比較結果に基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する。好適には、前記第1の画像ブロックおよび前記第2の画像ブロックは、それぞれ前記単位データを含み、画像データを所定の処理ブロックに分割し、空間領域から周波数領域に変換処理することにより得られる複数の変換係数を1組以上、含む変換ブロックである。好適には、前記第1の画像ブロックおよび前記第2の画像ブロックは、それぞれ前記単位データを含み、画像データを所定のDCTブロックに分割し、離散余弦変換(DCT)処理することにより得られる複数のDCT係数を1組以上、含むDCTブロックである。

【0029】[改変判定装置の作用] 本発明にかかる改変判定装置は、まず、処理の対象となるコンテンツデータを複数の部分に分割する。このコンテンツデータは、例えば、事故現場の音声データあるいは破損車両、器物などの画像データであって、意図的な改変が加えられると証拠として用いることができなくなる。次に、本発明にかかる改変判定装置は、上記分割の結果として得られたコンテンツデータの複数の部分それぞれに、改変の判定に用いられ、埋め込みの際に、他の部分へのデータの埋め込みに影響を与えず、また、改変の検出の際に他の部分からの影響を受けない所定の方式により、埋め込み

データ(いわゆる電子透かし(デジタルウォーターマーク))を埋め込込む。つまり、埋め込みデータは、コンテンツデータの複数の部分それぞれに、複数の部分それぞれに閉じた形で埋め込まれる。最後に、本発明にかかる改変判定装置は、コンテンツデータの上記複数の部分それぞれに閉じた形で埋め込まれた埋め込みデータを、上記複数の部分それぞれに閉じた処理により検出し、コンテンツデータのいずれの部分に改変が加えられたかを判定する。

【0030】[以下の説明において用いられる具体例] ここで、本発明にかかる改変判定装置が、画像データを分割し、分割した画像データに電子透かし(埋め込みデータ)を埋め込む方式は、分割した画像データそれぞれに閉じて行うことができる限り、どのようなものであってもよい。しかしながら、説明を明確化するためがあるので、以下、本発明にかかる改変判定装置が、例えば、JPEG方式により圧縮符号化された画像データを、それぞれDCT係数を複数組ずつ含む複数のセット(画像ブロック)に分割し、これらのセットそれぞれに対して、電子透かしを、セットごとに改変の判定が可能なように埋め込み、画像データが改変されたか否かの判定を、これらのセットごとに行う場合を具体例とする。また、本発明にかかる改変判定装置を、画像データの一部に対して埋め込みデータ(電子透かし)を埋め込み、改変の検出を行うようにしても、あるいは、埋め込みデータを埋め込んだ領域と、改変の検出を行う領域とが一致しないようにしてもよいが、以下、画像データの全部に埋め込みデータを埋め込み、改変を行う場合を具体例とする。また、本発明にかかる改変判定装置による埋め込みデータ(電子透かし)の埋め込みの対象となる上記DCT係数として、例えば、カラー画像データの輝度成分(Y)を、8×8画素構成の複数のDCTブロック(マクロブロック)にし、これらのDCTブロックをDCT処理して得られるDCT係数が用いられる場合を具体例とする。また、それぞれ複数組のDCT係数を含むセットを選択する方法としては、例えば、乱数を用いてランダムにDCT係数を選択してセットにする方法、あるいは、単純に隣り合ったDCT係数を選択してセットにする方法が考えられるが、以下、特に断らない限り、上記2例の後者の最も単純な場合、つまり、DCT係数のセットそれぞれが、単純に隣り合った2つのDCTブロックをDCT変換して得られる2組の(隣接した2つの)DCT係数を含むペアである場合を具体例として以下の説明を進める。

【0031】[データ付加装置の作用] 本発明にかかる改変判定装置において、データ付加手段は、画像データに対して、DCT係数のペアごとに改変の判定が可能なように、埋め込みデータ(電子透かし)の埋め込みを行う。

【0032】[画像分割手段] データ付加手段におい

て、画像分割手段は、例えば、JPEG方式により圧縮符号化された圧縮画像データをハフマン復号処理し、復号処理の結果として得られた画像データの3種類の成分の内、輝度成分(Y)のDCT係数を受け入れ、隣り合った2組のDCT係数同士に対応付け、対応付けた2組のDCT係数から構成されるペア(第1の画像ブロック)とする。

【0033】[埋め込みデータ付加手段]埋め込みデータ付加手段は、ペア(第1の画像ブロック)それぞれに含まれる2組のDCT係数の内の1つ以上(単位データ)を、相互に対応付けて取り出す(なお、2組のDCT係数それぞれから1つ以上取り出されるので、1つのペアからは複数の単位データが選択される)。また、埋め込みデータ付加手段は、例えば、鍵情報を用いて乱数を発生し、発生した乱数を用いて、例えば、96ビットの埋め込みデータをスクランブル処理する。また、埋め込みデータ付加手段は、ペア(第1の画像ブロック)それぞれと、スクランブルされた埋め込みデータ(第1の埋め込みデータ)の各ビットとを対応付ける。さらに、埋め込みデータ付加手段は、ペア(第1の画像ブロック)に含まれる2組のDCT係数それぞれから取り出され、これら2組のDCT係数の間で相互に対応するDCT係数(単位データ)同士の関係が、所定の規則に従って、これらのDCT係数が含まれていたペア(第1の画像ブロック)に対応付けられた埋め込みデータのビット(第1の埋め込みデータ)の値(1または0)を表すように、これらのDCT係数の値を調整することにより、埋め込みデータを埋め込む。なお、ペア(第1の画像ブロック)に含まれる2組のDCT係数から、DCT係数を選択する方法は、例えば、予め設定された固定の対応関係に基づいてDCT係数を選択する方法であっても、乱数に基づいてランダムにDCT係数に対応付けて選択する係数であってもよい。なお、以下、説明の明確化のために、特に断らない限り、各ペア(第1の画像ブロック)に含まれる2組のDCT係数それぞれから、ペアごとに乱数を用いてランダムに、互いに対応する3個ずつ(合計6個)のDCT係数を選択する場合、つまり、ペアが異なれば、異なった位置からDCT係数が選択されるが、同じペアに含まれるDCT係数からは、同じ位置のDCT係数が選択される場合を具体例にして説明を行う。

【0034】このように各ペアに、埋め込みデータのビットを埋め込むと、例えば、ハッシュ関数を用いて埋め込みデータを埋め込んだ場合と異なり、あるペアに対して加えられた改変は、そのペア以外に影響を与えない。つまり、このように埋め込みをおこなうと、画像の一部分に対する改変の影響は、画像の他の部分に及ばないので、画像に加えられた改変を、部分ごとに判定することができる。

【0035】[判定装置の作用]埋め込みデータ(第1

の埋め込みデータ)の各ビットが埋め込まれた後に、例えば、画像データの一部を塗りつぶし、写っていた物体が消去されるといった改変が加えられると、改変が加えられた部分のペア(第2の画像ブロック)に含まれ、相互に対応するDCT係数(単位データ)同士の関係が、上記所定の規則から外れることとなり、その埋め込みデータのビット(第2の埋め込みデータ)は、埋め込まれたときの埋め込みデータのビット(第1の埋め込みデータ)と異なる値を示すことになる。

【0036】また、例えば、96ビットの埋め込みデータ(第1の埋め込みデータ)を、1024ビット×768ビット構成の画像を構成する6144組のDCT係数のペア(第1の画像ブロック)に埋め込むと、埋め込みデータ(第1の埋め込みデータ)の各ビットが64回ずつ、1つの画像データに埋め込まれることになる。

【0037】一方、画像データの比較的、小面積の部分に対してのみ、改変が加えられた場合、改変が加えられた部分において、対応する埋め込みデータ(第1の埋め込みデータ)のビットを表さなくなるペアの数は、改変が加えられなかった部分において、対応する埋め込みデータ(第1の埋め込みデータ)のビットを表わしているペアの数よりも少なくなるはずである。

【0038】従って、改変が加えられた可能性がある画像から埋め込みデータ(第2の埋め込みデータ)を抽出し、抽出した埋め込みデータ(第2の埋め込みデータ)の内、埋め込みデータ(第1の埋め込みデータ)の同じビットに対応する64個のペア(第2の画像ブロック)それぞれが、上記所定の規則に従って、1、0いずれの値を表しているかの多数決を採ると、多数のペアが表している値を、データ付加装置が付加した埋め込みデータ(第1の埋め込みデータ)の値であると判断することができる。同様に、この多数決の結果、少数となったペア(第2の画像ブロック)の位置に、改変が加えられたと推定することができる。

【0039】本発明にかかる判定装置は、このような埋め込みデータの性質を利用し、改変が加えられた可能性があるDCT係数のペア(第2の埋め込みデータ)それぞれから、改変が加えられた結果、埋め込まれた当初とは値が変更されている可能性がある埋め込みデータ(第2の埋め込みデータ)を抽出する。さらに、判定装置は、この抽出結果に基づいて、DCT係数のペア(第2の画像ブロック)のいずれに改変が加えられているか、つまり、画像データのいずれの部分に改変が加えられているかを判定する。

【0040】[埋め込みデータ抽出手段]埋め込みデータ抽出手段は、本発明にかかるデータ付加装置により埋め込みデータ(第1の埋め込みデータ)が埋め込まれた後に改変が加えられた可能性があるペア(第2の画像ブロック)の2組のDCT係数それぞれに含まれ、相互に対応するDCT係数(単位データ)が、上記所定の規則

に従って表す値(第2の埋め込みデータ)を抽出する。

【0041】[改変判定手段] 改変判定手段は、埋め込みデータの同じビットに対応する複数のペア(第2の画像ブロック)が、1, 0いずれの値を表すかの多数決を採り、多数のペアが表す値を、埋め込み時の埋め込みデータ(第1の埋め込みデータ)と判定し、この埋め込みデータと異なる値を表すペア(第2の画像ブロック)に対して、改変がなされたと判定する。

【0042】[データ付加装置] 本発明にかかるデータ付加装置は、画像データに対して改変が加えられたか否かを判定するために、画像データに所定の埋め込みデータを付加するデータ付加装置であって、前記判定は、前記画像データに含まれる複数の第2の画像ブロックそれぞれに付加された第2の埋め込みデータに基づいて、前記画像ブロックそれぞれに改変が加えられたか否かを判断することにより行われ、前記データ付加装置は、画像データを複数の第1の画像ブロックに分割する画像分割手段と、分割の結果として得られた前記複数の第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、前記複数の第2の画像ブロックとする埋め込みデータ付加手段とを有する。

【0043】[判定装置] また、本発明にかかる判定装置は、画像データを複数の第1の画像ブロックに分割し、分割の結果として得られた前記第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加することにより作られた複数の第2の画像ブロックそれぞれに改変が加えられたか否かを判定する判定装置であって、前記第2の画像ブロックそれぞれに付加された埋め込みデータ(第2の埋め込みデータ)を抽出する埋め込みデータ抽出手段と、抽出された前記第2の埋め込みデータに基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定手段とを有する。

【0044】[改変判定方法] 本発明にかかる改変判定方法は、所定の埋め込みデータを埋め込む対象となるコンテンツデータに前記埋め込みデータを付加し、前記所定の埋め込みデータが埋め込まれたコンテンツデータに対して改変が加えられたか否かを判定するコンテンツ改変判定方法であって、前記コンテンツデータを複数の第1のブロックに分割し、分割の結果として得られた前記複数の第1のブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、複数の第2のブロックとし、前記第2のブロックそれぞれに付加された前記埋め込みデータ(第2の埋め込みデータ)を抽出し、抽出された前記第2の埋め込みデータに基づいて、前記第2のブロックそれぞれに改変が加えられたか否かを判定する。

【0045】[記録媒体] また、本発明にかかる第1の記録媒体は、画像データに所定の埋め込みデータを付加するデータ付加装置と、前記所定の埋め込みデータが埋

め込まれた画像データに対して改変が加えられたか否かを判定する判定装置とを有する改変判定装置において、画像データを複数の第1の画像ブロックに分割する画像分割ステップと、分割の結果として得られた前記複数の第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、複数の第2の画像ブロックとする埋め込みデータ付加ステップと、前記第2の画像ブロックそれぞれに付加された埋め込みデータ(第2の埋め込みデータ)を抽出する埋め込みデータ抽出ステップと、抽出された前記第2の埋め込みデータに基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定ステップとをコンピュータに実行させるプログラムを記録する。

【0046】また、本発明にかかる第2の記録媒体は、画像データに対して改変が加えられたか否かを判定するために、画像データに所定の埋め込みデータを付加するデータ付加装置において、前記判定は、前記画像データに含まれる複数の第2の画像ブロックそれぞれに付加された第2の埋め込みデータに基づいて、前記画像ブロックそれぞれに改変が加えられたか否かを判断することにより行われ、画像データを複数の第1の画像ブロックに分割する画像分割ステップと、分割の結果として得られた前記複数の第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、前記複数の第2の画像ブロックとする埋め込みデータ付加ステップとをコンピュータに実行させるプログラムを記録する。

【0047】また、本発明にかかる第3の記録媒体は、画像データを複数の第1の画像ブロックに分割し、分割の結果として得られた前記第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加することにより作られた複数の第2の画像ブロックそれぞれに改変が加えられたか否かを判定する判定装置において、前記第2の画像ブロックそれぞれに付加された埋め込みデータ(第2の埋め込みデータ)を抽出する埋め込みデータ抽出ステップと、抽出された前記第2の埋め込みデータに基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定ステップとをコンピュータに実行させるプログラムを記録する。

【0048】

【発明の実施の形態】 以下、本発明の実施形態を説明する。

【0049】[改変判定装置1] 図1は、本発明にかかる改変判定方法を実現する画像改変判定装置1の構成を示す図である。図1に示すように、画像改変判定装置1は、CRT表示装置あるいは液晶表示装置等の表示装置100、キーボードおよびマウス等を含む入力装置102、デジタルカメラインターフェースIF(カメラIF)104、メモ리카ードインターフェース(メモ리카ードIF)106、MO装置およびCD装置等の記憶装置108、および、メモリ112およびマイクロプロセ

ッサ(CPU)114等を含むコンピュータ本体(PC本体)110から構成され、必要に応じて、さらに通信装置116が付加される。つまり、画像改変判定装置1は、一般的なコンピュータに、カメラIF104およびメモ리카ードIF106を付加した構成を採る。

【0050】画像改変判定装置1は、これらの構成部分により、光磁気ディスク(MO)あるいはコンパクトディスク(CD)等の記録媒体120に記録されて記憶装置108に供給される埋込・判定プログラム2(図2を参照して後述する)を、メモリ112にロードして実行し、画像データに対する電子透かし(埋め込みデータ)の埋め込み処理および改変(人為的に加えられた改変か、データが壊れる等の事故に起因する改変かを問わない)の判定処理を実行する。

【0051】つまり、画像改変判定装置1は、デジタルカメラ140が撮影した画像を、例えばJPEG方式により圧縮符号化して生成した圧縮画像データを、カメラIF104を介して受け入れる。あるいは、画像改変判定装置1は、デジタルカメラ140がメモ리카ード142に記録した圧縮画像データを、メモ리카ードIF106を介して受け入れる。圧縮画像データを受け入れると、画像改変判定装置1は、圧縮画像データに電子透かし(埋め込みデータ)を埋め込み、埋め込んだ電子透かし(埋込データ)を用いて、圧縮画像データのいずれの部分に改変が加えられたかを判定する。

【0052】[埋込・判定プログラム2]図2は、図1に示した画像改変判定装置1が実行し、本発明にかかる改変判定方法を実現する埋込・判定プログラム2の構成を示す図である。図2に示すように、埋込・判定プログラム2は、埋込・抽出部3、鍵情報データベース(DB)22および画像データベース(DB)24から構成され、埋込・抽出部3は、埋込データ生成部20、制御部26、埋込部30、抽出部40およびOS50から構成される。

【0053】[OS50]OS50は、例えば、ウィンドウズ(マイクロソフト社商標)等のオペレーティングシステムソフトウェアであって、埋込・判定プログラム2の各構成部分の実行制御を行う。また、OS50は、埋込データ生成部20に対して、メモ리카ード142のシリアル番号および時刻等、電子透かし(埋込データ)の生成に必要なデータを供給するなど、埋込・判定プログラム2の各構成部分の処理に必要とされるデータを供給する。

【0054】[制御部26]制御部26は、例えば、表示装置100に操作用のGUI画像(図示せず)を表示し、表示されたGUI画像に対するユーザの操作を受け入れ、必要に応じて、受け入れた操作を示す操作データを、埋込・判定プログラム2の各構成部分に供給する。また、制御部26は、受け入れたユーザの操作に応じて、埋込・判定プログラム2の各構成部分の動作を制御

する。

【0055】[画像DB24]画像DB24は、埋込部30が埋め込みデータを埋め込んだ圧縮画像データ(JPEGデータ)を記憶装置108に挿入された記録媒体120、あるいは、メモ리카ードIF106に挿入されたメモ리카ード142に記憶・管理し、記憶・管理した画像データを読み出して抽出部40に対して出力する。

【0056】[鍵情報DB22]鍵情報DB22は、画像DB22が管理するJPEGデータと、埋込部30が、このJPEGデータへ埋め込みデータを埋め込む際に、乱数を発生させるために用いる鍵(例えば64ビットの数値)とを対応付けた鍵情報を記憶装置108等に記憶・管理し、記憶・管理した鍵情報を読み出して埋込部30および抽出部40に対して出力する。

【0057】[埋込データ生成部20]埋込データ生成部20は、例えば、OS50から入力されるメモリのシリアル番号といったデータから、96ビットの埋め込みデータを生成し、埋込部30に対して出力する。

【0058】[埋込部30]図3は、図2に示した埋込部30の構成を示す図である。図4は、図3に示したデータ埋込部32の構成を示す図である。図3および図4に示すように、埋込部30は、復号部300、データ埋込部32および符号化部304から構成され、データ埋込部32は、画像分割部320、乱数発生部322、位置決め部324、スクランブル部326および係数操作部328から構成される。

【0059】[埋込部30の概要]埋込部30は、これらの構成部分により、まず、カラーの圧縮画像データを構成するクロマ成分Cb、Crおよび輝度成分Yの1組8画素×8画素構成(1組64画素)のDCT係数の内、例えば輝度成分YのDCT係数を、それぞれDCT係数2組ずつを含む複数のペア(第1の画像ブロック)とする。

【0060】埋込部30は、さらに、これらのペアそれぞれに、埋込データ生成部20が発生した96ビットの埋込データを、鍵情報DB22(図2)から供給された鍵情報を用いて、例えば16ビットの線形合同法により発生した乱数に基づいてスクランブルしたデータ(第1の埋め込みデータ;以下、記述の簡略化のために、このように「スクランブルされた埋め込みデータ」を、単に「埋め込みデータ」とも記す)の各ビットを埋め込む。

【0061】[埋込部30の詳細]図5～図12をさらに参照して、埋込部30の処理の詳細を説明する。図5は、デジタルカメラ140(図1)が撮影した非圧縮画像データを例示する図である。図6(A)は、図5に例示した非圧縮画像データの一部を示す図であり、

(B)は、(A)に例示した非圧縮画像データ(部分)に含まれるDCTブロック(マクロブロック)を示す図であり、(C)は、(B)に示したDCTブロックそれぞれに含まれる8×8構成の画素を示す図である。

【0062】なお、本来、DCTブロックと、8×8構成のDCT係数とは区別する必要があるが、記述の簡略化のために、以下、特に断らない限り、8×8構成のDCT係数をDCTブロックとも記し、8×8構成のDCTブロックに含まれる各DCT係数を、DCT係数と記す。

【0063】デジタルカメラ140(図1)は、例えば、人物および風景を撮影し、図5に例示した非圧縮カラー画像データを生成し、さらに、JPEG方式により圧縮符号化する。つまり、デジタルカメラ140は、図6(A)～(C)に例示するように、得られた非圧縮画像データに含まれる輝度成分Yおよびクロマ成分Cr、Cbそれぞれを、それぞれ8×8(64)個の画素を含むDCTブロック(マクロブロックともいう)に分割し、分割の結果として得られたDCTブロックをDCT変換し、さらに、ハフマン符号化して、JPEG方式の圧縮画像データを生成し、カメラIF104を介して、あるいは、メモリカード142およびメモリカードIF106を介して、PC本体110(図1)により実行される埋込・判定プログラム2の埋込部30(図2, 3)に対して出力する。

【0064】図7(A)は、デジタルカメラ140から入力される圧縮画像データを復号部300がハフマン復号して得られる輝度信号YのDCT係数を示す図であり、(B)は、(A)に示した輝度信号YのDCT係数の内、それぞれ隣り合う2組を対応付ける方法を示す図であり、(C)は、(B)に示した方法により対応付けられたDCT係数のペアを示す図である。

【0065】埋込部30は、まず、入力されたJPEG方式の圧縮画像データをハフマン復号して輝度成分Yおよびクロマ成分Cr、CbのDCTブロックを得て、得られたこれらのDCTブロックの内、図7(A)に示す輝度成分Yの12288個のDCTブロック(1, 1～96, 128)を、図7(B), (C)に示すように、隣り合う2つ(ブロック1, 2)同士で6144(12288/2)個のペアにする。埋込部30は、このようにして得られた6144(96×64)個のペアそれぞれに、上述のように乱数によりスクランブルされた96ビットの埋め込みデータの各ビットを、64回ずつ繰り返し対応付ける。

【0066】図8は、図2, 3に示した埋込部30が1

$$(A_1 < A_2 \& \& B_1 < B_2 \& \& C_1 < C_2) \parallel$$

$$(A_1 > A_2 \& \& B_1 > B_2 \& \& C_1 < C_2) \parallel$$

$$(A_1 < A_2 \& \& B_1 > B_2 \& \& C_1 > C_2) \parallel$$

$$(A_1 > A_2 \& \& B_1 < B_2 \& \& C_1 > C_2) \parallel$$

ペアに対応付けられた埋め込みデータのビットの値が0

$$(A_1 < A_2 \& \& B_1 < B_2 \& \& C_1 < C_2) \parallel$$

$$(A_1 > A_2 \& \& B_1 < B_2 \& \& C_1 < C_2) \parallel$$

$$(A_1 < A_2 \& \& B_1 > B_2 \& \& C_1 < C_2) \parallel$$

つのペア(図7(A), (B))に含まれるDCTブロック(ブロック1, 2)それぞれから選択した相互に対応するDCT係数を例示する図である。なお、図8は、ペア*i*(1 ≤ *i* ≤ 6144)に含まれる2つのDCTブロック(ブロック1, 2)それぞれから、同じ位置の3個のDCT係数(2, 3), (3, 2), (3, 3)が選択された場合を例示する。

【0067】埋込部30は、例えば、鍵情報DB22(図2)から供給された鍵を用いて上述のように生成した乱数を用いて、図8に示すように、DCTブロック(ブロック1, 2)内の相互に対応する3つのDCT係数(A₁, A₂, B₁, B₂, C₁, C₂; 単位データ)を、ペアごとにランダムに選択する。言い換えると、埋込部30は、任意の一つのペアに含まれるDCTブロック(ブロック1, 2)では、同じ位置のDCT係数をビットの埋め込みのために選択するが、これと異なるペアのDCTブロックでは、異なる位置のDCT係数を選択する。

【0068】図9(A), (B)は、図8に例示したように選択されたブロック1, 2それぞれのDCT係数を、埋め込みデータのビット(値1)を埋め込むために、DCT係数の数値を変更する必要がある場合について例示する図である。図10は、図8に例示したように選択されたブロック1, 2それぞれのDCT係数を、埋め込みデータのビット(値1)を埋め込むために、DCT係数の数値を変更する必要がない場合について例示する図である。

【0069】埋込部30は、例えば、図8に例示したように、ペア*i*の2つのDCTブロック(ブロック1, 2)から選択した相互に対応するDCT係数(A₁, A₂, B₁, B₂, C₁, C₂)値同士の関係が、図9(A), (B)および図10に例示するように、上述のようにペアそれぞれに対応付けられた埋め込みデータのビットの値に応じて、下表1に例示する規則(規則1-1, 1-2)に従うように調整することにより、各ペアに、対応する埋め込みデータのビットの値(1, 0)を埋め込む。

【0070】

【表1】表1: DCT係数の関係を示す規則: ペアに対応付けられた埋め込みデータのビットの値が1である場合:

... (規則1-1)

である場合:

$$(A_1 > A_2 \&\& B_1 > B_2 \&\& C_1 > C_2)$$

ただし、上記規則1-1, 1-2において、 $X \&\& Y$ は、条件 X, Y の両方を満たすことを示し、 $X || Y$ は、条件 X, Y のいずれかを満たすことを示す。

【0071】例えば、図9(A)に例示するように、ペア i に対応付けられた埋め込みデータのビットの値が1であり、ペア i の2つのDCTブロック(ブロック1, 2)の相互に対応するDCT係数($A_1, A_2, B_1, B_2, C_1, C_2$)の値が、それぞれ4, 4, 2, 3, 5, 4である場合、これらのDCT係数の値の関係は、 $A_1 = A_2$ であるため、上記規則1-1, 1-2のいずれをも満たさない。

【0072】そこで、埋込部30は、図9(B)内の数字に丸印を付して例示するように、相互に対応するDCT係数($A_1, A_2, B_1, B_2, C_1, C_2$)同士の値の関係が、上記規則1-1の($A_1 < A_2 \&\& B_1 < B_2 \&\& C_1 < C_2$)の条件を満たすことになるように、 A_2 の値を増やして、値1の埋め込みデータのビットを埋め込む。つまり、例えば、値1のビットを埋め込む場合に、DCT係数($A_1, A_2, B_1, B_2, C_1, C_2$)同士の値が規則1-1を満たさない場合には、常に、これらのDCT係数同士の関係が、上記規則1-1の内、($A_1 < A_2 \&\& B_1 < B_2 \&\& C_1 < C_2$)の条件を満たすことになるように、DCT係数を調節して、値1の埋め込みデータのビットを埋め込む。

【0073】また、例えば、図10に例示するように、ペア i に対応付けられた埋め込みデータのビットの値が1であり、ペア i の2つのDCTブロック(ブロック1, 2)の相互に対応するDCT係数($A_1, A_2, B_1, B_2, C_1, C_2$)の値が、それぞれ3, 5, 6, 3, 5, 4である場合、これらのDCT係数の値の関係は、上記規則1-1の条件($A_1 < A_2 \&\& B_1 > B_2 \&\& C_1 > C_2$)を満たしている。従って、この場合には、埋込部30は、ペア i の2つのDCTブロック(ブロック1, 2)のDCT係数($A_1, A_2, B_1, B_2, C_1, C_2$)の値を変更しない。

【0074】図11は、埋込部30(図2, 3)が、DCTブロックに対して埋め込みデータを埋め込むために用いられる埋め込みテーブルを例示する図表である。なお、図11には、埋め込みデータビット欄が現れているが、この欄は、埋め込みデータがスクランブル処理されていることを説明するために示したものであり、実際の処理においては用いられない。ここまで説明した埋込部30の埋め込み処理を、さらに図11を参照して説明する。埋込部30は、1024画素×768画素構成の画像データ(図5, 6(A)~(C))から得られた12288個のDCTブロックの内、隣り合った2つのDCTブロック同士を対応付けて(図7(A)~(C))、6144個のペアを作る。

【0075】また、埋込部30は、埋込データ生成部2

... (規則1-2)

0(図2)から供給される96ビットの埋め込みデータを、鍵情報DB22から供給される鍵から作成した乱数でスクランブル処理し、スクランブル処理した96ビットの埋め込みデータのビットそれぞれの値(1, 0)を、下記方法により64回ずつ6144個のペアそれぞれに対応付け、図11に示すように、埋め込みテーブルの埋め込みデータ割り当て欄に書き込む。

【0076】[埋め込みデータの対応付け方法]なお、図11に例示するように、連続した96ペアごとに、それぞれ異なった順番にスクランブルされた96ビットの埋め込みデータの各ビットが対応付けられるので、例えば、第5番目のペアと、第160番目のペアに、埋め込みデータの第7番目のビット(1)が割り当てられる。以下、同様に、6144個のペアを、順番に64組×96ペアに分割して得られる各組ごとに異なる順番で、各組に含まれる96ペアそれぞれに、96ビットの埋め込みデータの各ビットが対応付けられる。

【0077】例えば、96ビットの埋め込みデータの第1~第4ビットはそれぞれ、第1~第96ペアを含む第1組においては、第11ペア、第5ペア、第31ペアおよび第9ペアに対応付けられ、第97~第192ペアを含む第2組においては、第99ペア、第126、第100ペア、第153ペアに対応付けられる(後に図18に例示)。

【0078】また、埋込部30は、上述のように生成された乱数を用いて、図8に例示したように、ペアごとに、2つのDCTブロック(ブロック1, 2)からいずれのDCT係数($A_1, A_2, B_1, B_2, C_1, C_2$)を取り出すかを決め、取り出したDCT係数の値を、埋め込みテーブルのブロック1, 2の欄に書き込む。上述のように、埋込部30が8×8構成のDCT係数のいずれを取り出すかは、ペアごとに一定ではない。

【0079】以上の処理が終了すると、埋込部30は、各ペアのDCTブロック(ブロック1, 2)から選択されたDCT係数($A_1, A_2, B_1, B_2, C_1, C_2$)が、上記表1に示した規則1-1, 1-2に基づいて、埋め込みテーブルの埋め込みデータ割り当て欄のビットの値を表すように、埋め込みテーブルのブロック1, 2の欄に書き込まれたDCT係数($A_1, A_2, B_1, B_2, C_1, C_2$)の値を操作する。

【0080】埋込部30は、ここまで説明したように埋め込みデータが埋め込まれた輝度成分YのDCT係数(DCTブロック)と、クロマ成分 C_r, C_b のDCT係数を、再びハフマン符号化して、JPEG方式により伸長可能な圧縮画像データ(JPEGデータ)として、画像DB24(図2)に対して出力する。

【0081】[埋込部30の構成部分]再び図3, 4を参照して、埋込部30の構成部分を説明する。

【0082】[復号部300] 復号部300 (図3) は、制御部26 (図2) の制御に従って、カメラIF104またはメモ리카ードIF106を介して供給されるJPEGデータをハフマン復号し、復号の結果として得られる3種類のDCT係数(DCTブロック)の内、2種類のクロマ成分Cr, CbのDCT係数(DCTブロック)を、符号化部304に対して出力し、輝度成分YのDCT係数(DCTブロック)を、データ埋込部32に対して出力する。

【0083】[データ埋込部32] データ埋込部32は、図7~図11を参照して説明した埋め込みデータの埋め込み処理を行う。以下、図4を参照して、データ埋込部32の各構成部分を説明する。

【0084】[画像分割部320] 画像分割部320は、復号部300から入力される輝度信号YのDCT係数(DCTブロック; 図7(A))を、図7(B), (C)に示したペアに分割して、係数操作部328に対して出力する。

【0085】[乱数発生部322] 乱数発生部322は、鍵情報DB22 (図2) から入力される例えば64ビットの鍵を用いて、16ビットの線形合同法により乱数を発生し、発生した乱数RNを位置決め部324およびスクランブル部326に対して出力する。

【0086】[位置決め部324] 位置決め部324は、画像分割部320が作成したペアそれぞれにおいて、乱数発生部322から入力される乱数RNを用いて、2つのDCTブロック(ブロック1, 2)のいずれのDCT係数を選択するか(選択するDCT係数の位置; 図8)を決定し、決定したDCT係数の位置を示す位置データを係数操作部328に対して出力する。

【0087】[スクランブル部326] スクランブル部326は、乱数発生部322から入力される乱数RNを用いて、埋込データ生成部20 (図2) から入力される96ビットの埋め込みデータをスクランブル処理する。このスクランブル部326のスクランブル処理により、96ビットを1つの繰り返し単位とし、繰り返し単位ごとに異なった順番で96ビットの埋め込みデータの全てのビットを含み、この繰り返し単位を64個含むデータ(スクランブルされた埋め込みデータ、以下、単に埋め込みデータとも記す)を係数操作部328に対して出力する。

【0088】[係数操作部328の埋め込みテーブル作成処理] 係数操作部328は、まず、図11に示した埋め込みテーブルを作成する。つまり、まず、係数操作部328は、位置決め部324から入力された位置データに基づいて、各ペアの2つのDCTブロック(ブロック1, 2; 図7(B)等)からDCT係数を取り出し(図8)、埋め込みテーブル(図11)のブロック1, 2の欄に書き込み、さらに、スクランブル部326から入力された埋め込みデータを埋め込みテーブルの埋め込みデ

ータの割り当て欄に書き込む。

【0089】[係数操作部328のデータ埋め込み処理] 図12は、図4に示した係数操作部328が、DCTブロックのペアに埋め込みデータを埋め込む処理(S10)を示す図である。次に、係数操作部328は、DCT係数(DCTブロック)のペアそれぞれに、埋め込みテーブル(図11)において対応付けられた埋め込みデータのビットを埋め込み、埋め込みデータを埋め込んだ輝度成分のDCT係数Y'として符号化部304 (図3)に対して出力する。

【0090】図12に示すように、係数操作部328は、ステップ100 (S100)において、6144個のペアを示す変数iを1に初期設定する。

【0091】ステップ102 (S102)において、係数操作部328は、第i番目のペアの操作対象となるDCT係数(A₁, A₂, B₁, B₂, C₁, C₂)を、埋め込みテーブル(図11)のブロック1, 2欄から、埋め込むビットを、同じく埋め込みテーブルの埋め込みデータ割り当て欄から取り出す。

【0092】ステップ104 (S104)において、係数操作部328は、S102の処理において取り出した埋め込みビットの値が1であるか否かを判断し、埋め込みビットの値が1である場合にはS106の処理に進み、0である場合にはS110の処理に進む。

【0093】ステップ106 (S106)において、係数操作部328は、操作対象のDCT係数が、表1に示した規則1-1を満たすか否か、つまり、操作対象のDCT係数が1を表すか判断し、図10に例示したように、規則1-1を満たす場合にはS114の処理に進み、これ以外の場合にはS108の処理に進む。

【0094】ステップ108 (S108)において、係数操作部328は、操作対象のDCT係数が、規則1-1を満たすように操作する。

【0095】ステップ110 (S110)において、係数操作部328は、操作対象のDCT係数が、表1に示した規則1-2を満たすか否か、つまり、操作対象のDCT係数が0を表すか否かを判断し、規則1-2を満たす場合にはS114の処理に進み、これ以外の場合にはS112の処理に進む。

【0096】ステップ112 (S112)において、係数操作部328は、操作対象のDCT係数が、規則1-2を満たすように操作する。

【0097】ステップ114 (S114)において、係数操作部328は、変数iが6144であるか否か、つまり、全てのペアに対して埋め込みデータの埋め込み処理が終了したか否かを判断し、終了した場合には処理を終了し、これ以外の場合には変数iを1増やしてS102の処理に戻る。

【0098】[符号化部304] 符号化部304 (図3) は、復号部300から入力されたクロマ成分Cr,

CbのDCT係数と、データ埋込部32から入力され、埋め込みデータが埋め込まれた輝度成分YのDCT係数Y'とをハフマン符号化し、画像DB22に対して出力する。

【0099】[抽出部40]図13は、図2に示した抽出部40の構成を示す図である。図14は、図13に示した埋め込みデータ抽出部42の構成を示す図である。図13および図14に示すように、抽出部40は、復号部400、画像分割部402、符号化部404、画像合成部406、埋込データ抽出部42、改変検出部44およびクラスタリング部46から構成され、埋込データ抽出部42は、乱数生成部420、位置決め部422、抽出順序生成部424、対応付け部426およびデータ抽出部428から構成される。

【0100】[抽出部40の概要]埋込部30により、図7～図12を参照して上述したように埋め込みデータが埋め込まれたJPEGデータの一部分または全部に対して、その後、改変が加えられると、各ペアの2つのDCTブロック(ブロック1, 2; 図7(B)等)の間で相互に対応し、埋め込みデータの埋め込みに用いられたDCT係数($A_1, A_2, B_1, B_2, C_1, C_2$; 図8等)の値の関係が、上記表1に示した規則1-1, 1-2に従って、図9(A), (B)および図10に例示した処理により埋め込まれたビットの値を示さなくなる。

【0101】抽出部40は、上述した構成部分により、埋め込みデータが埋め込まれたJPEGデータのこのような性質を利用して、埋込部30が生成したJPEGデータに改変が加えられたか否か、および、改変が加えられた場合には、画像データ(図5)のいずれの部分に改変が加えられたかを判定し、表示する。

【0102】[抽出部40の詳細]以下、図15～図22をさらに参照して、抽出部40の処理を詳細に説明する。上述したように、埋込部30(図2, 3)においては、各ペアにおいて、埋め込みデータの埋め込みに用いられるDCT係数の位置は、同じく、鍵情報DB22から供給された鍵から生成された乱数によって求められる。従って、抽出部40においても、埋込部30と同じ鍵を使うことにより、各ペアのDCTブロック(ブロック1, 2; 図8)において、いずれのDCT係数が、埋め込みデータの埋め込みに用いられたかを知ることができる。

【0103】また、埋込部30においては、96ビットの埋め込みデータの各ビットは、鍵情報DB22から供給される鍵から生成された乱数によってスクランブルされ、各ペアに対応付けられている。従って、抽出部40においても、埋込部30と同じ鍵を使うことにより、いずれのペアに、96ビットの埋め込みデータのいずれのビットが対応付けられたかを知ることができる。

【0104】抽出部40は、このように、埋込部30と同じ鍵を用いて、各ペアの2つのDCTブロック(ブ

ロック1, 2)において、いずれのDCT係数がビットの埋め込みに用いられたかを知り、さらに、ビットの埋め込みに用いられた相互に対応するDCT係数同士の値の関係が、上記表1に示した規則1-1, 1-2のいずれに該当するかによって、各ペアに埋め込まれた埋め込みデータのビットの値(1, 0)を抽出する。次に、抽出部40は、埋込部30と同じ鍵を用いて、各ペアから抽出された埋め込みデータのビットの値が、埋め込みデータのいずれのビットに対応するかを判定する。

【0105】図15(A)は、埋込部30(図2, 3)が埋め込みデータを埋め込んだJPEGデータを伸長した画像を例示する図であり、(B)は、(A)に示した画像のなかで改変を行う個所の例示であり、(C)は、改変後の画像を例示する図である。ここで、例えば、埋込部30が、図5および図6(A)～(C)に示した画像データから得られたJPEGデータに対して、図7～図12に示したように埋め込みデータを埋め込んで生成したJPEGデータを、誰かが伸長し、図15(A)に例示する画像を得て、図15(B)に点線で示す個所に改変を加え、図15(C)に示すように、画像中の車の部分消去/修正した画像を生成し、再度、JPEG方式で圧縮符号化し、元のJPEGデータと置き換えたすると、改変は画像のごく一部に加えられたため、埋め込みデータの同一のビットに対応付けられた64個のペアから抽出された64の値の多くは、改変前の値を示し、少数だけが改変によって変更された値を示すはずである。

【0106】抽出部40は、画像の一部に変更が加えられた場合のこのような性質を利用して、各ペアから抽出したビットを、埋め込みデータの各ビットに対応付けて多数決を採り、埋め込みデータの第kビットに対応する64個のペアの多数から値1(0)が抽出され、少数のペアから値0(1)が抽出された場合には、埋込部30が、これら64個のペアに、第kビットとして、値1(0)を埋め込んだと推定する。つまり、抽出部40は、埋め込みデータの各ビットについて、抽出された値の多数決を採り、埋込部30が各ペアに埋め込んだ埋め込みデータのビットの値を推定するとともに、多数決の結果、少数となった値が抽出されたペアに対して、改変が加えられたと判定する。

【0107】図16は、改変が加えられた部分を示す2値画像を、元の画像と合成して示す画像を例示する図である。さらに、抽出部40は、例えば、図16に示すように、改変が加えられたペアを示す2値画像(図16の中央付近とナンバープレート部の網掛け部分)と、図5に示した元の画像とを合成して、いずれの部分に改変が加えられたかを表示装置100(図1)等に表示する。

【0108】図17は、クラスタリング処理により、改変が加えられた範囲を示す画像を、元の画像と合成して示す画像を例示する図である。あるいは、抽出部40

は、例えば、図17に示すように、クラスタリング処理により、図16に示した2値画像のモザイク状の部分が存在する範囲を示す画像(図17左上の長方形)を得て、この画像と、図5に示した元の画像とを合成して、いずれの範囲に改変が加えられたかを表示装置100等に表示する。

【0109】このような処理を行うために、まず、抽出部40は、画像DB22から供給されるJPEGデータをハフマン復号し、得られた3種類のDCT係数(DCTブロック)の内、輝度成分Yの12288個のDCT係数(DCTブロックY')を取り出し、隣り合ったDCT同士を、図7(B)、(C)に示したように、6144個のペアにする。

【0110】抽出部40は、これらのペアそれぞれに含まれる2つのDCTブロック(ブロック1、2;図8)の埋め込みデータの埋め込みに用いられたDCT係数の関係が、上記表1に示した規則1-1、1-2のいずれに該当するかを判断し、各ペアに埋め込まれた埋め込みデータ(第2の埋め込みデータ)のビットの値(1、0)を抽出する。もし、2つのDCTブロック(DCTブロック1、2)の対応するDCT係数が等しい場合(例えば、 $A_1=A_2$)には、この関係は規則1-1、1-2のいずれにも当てはまらないため、抽出部40は、直ちにこのペアに改変が加えられたと判断することができる。なお、以下、説明の明確化のために、対応するDCT係数が等しくない場合を具体例とする。

【0111】図18は、埋込部30(図2、3)が生成したJPEGデータに、改変・誤りが加えられていない場合に、抽出部40が改変等がなされていないJPEGデータに含まれる各ペアから抽出するビットの値を示す図である。抽出部40が、埋込部30が生成した後、改変も誤りも加えられていないJPEGデータに含まれる各ペア(第2の画像ブロック)から抽出した埋め込みデータのビットの値を、図18に示すように、各ペアに、埋め込みデータのいずれのビットが対応付けられているかに従って並べると、各埋め込みデータに対応するペアから抽出された全てのビットの値は一致する。

【0112】図19は、埋込部30(図2、3)が生成したJPEGデータに、改変・誤りが加えられた場合に、抽出部40が改変等がなされたJPEGデータに含まれる各ペアから抽出するビットの値を例示する図である。一方、例えば、抽出部40が、埋込部30が生成した後、改変等が加えられたJPEGデータに含まれる各ペア(第2の画像ブロック)から抽出した埋め込みデータのビットの値を、図18と同様に、各ペアに、埋め込みデータのいずれのビットが対応付けられているかに従って並べると、図19に示すように、改変が加えられた部分の少数のペアから抽出されたビットは、図19中に太枠を付した値として示すように、改変が加えられていない他の多数のペアから抽出されたビットと異なる値を

採り、不整合を生じる。抽出部40は、このようにして多数決により得られたビットの値を、埋込部30が埋め込んだ埋め込みデータのビットの値と推定する。

【0113】図20は、抽出部40(図13、14)が、図15に例示したように改変が加えられたJPEGデータから、図19に例示したように改変等が加えられたペアを判定し、改変が加えられたペアの画像内における位置を示す2値画像を例示する図である。なお、説明の都合上、図20に示した例と、図15等に示した例とは、必ずしも一致しない。このように、抽出部40は、図20に例示するように、多数決により推定された値と異なる値のビットが抽出されたペアが、画面内のいずれに位置するかを示す2値画像を生成する。なお、抽出部40が生成した2値画像は、図16を参照して上述したように、元の画像と合成され、表示装置100(図1)等に表示される。

【0114】図21(A)~(D)は、抽出部40(図13、14)が、図15に例示したように改変が加えられたJPEGデータから、図19に例示したように改変等が加えられたペアを判定し、改変が加えられたペアが画像内において、いずれの範囲に存在するかを示すクラスタリング画像を例示する図である。なお、説明の都合上、図21(A)~(D)に示した例と、図15等に示した例とは、必ずしも一致しない。また、抽出部40は、図21(A)、(C)にそれぞれ例示するように、多数決により推定された値と異なる値のビットが抽出されたペアが、画面内のいずれの範囲に存在するかを判定し、それぞれ図21(B)、(D)に例示するクラスタリング画像を生成する。なお、抽出部40が生成したクラスタリング画像は、図17を参照して上述したように、元の画像と合成され、表示装置100(図1)等に表示される。

【0115】[抽出部40の構成部分]以下、再び図13、14を参照して、抽出部40の各構成部分を説明する。

【0116】[復号部400]復号部400は、操作に応じた制御部26の制御に従って、画像DB22から供給されるJPEGデータをハフマン復号し、復号の結果として得られた3種類の画像成分の内、クロマ成分Cr、Cbを符号化部404に対して出力し、輝度成分Y'を、画像分割部402に対して出力する。

【0117】[画像分割部402]画像分割部402は、復号部400から入力された輝度成分Y'を、DCT係数(DCTブロック)単位に分割し、分割の結果として得られたDCT係数(DCTブロック)を、埋込データ抽出部42に対して出力する。

【0118】[埋込データ抽出部42]埋込データ抽出部42は、画像分割部402から入力された輝度成分Y'のDCTブロックを2つずつ対応付けて、埋込部30においてと同様なペア(図7(B)、(C)および図

8等)とし、これらのペアに埋め込まれた埋め込みデータのビットの値を抽出し、図18、19に例示した形式の抽出データとして改変検出部44に対して出力する。また、埋込データ抽出部42は、画像分割部402から入力された輝度成分Y'をそのまま、輝度成分Yとして符号化部404に対して出力する。

【0119】[対応付部426] 対応付部426(図14)は、画像分割部402から入力された12288個のDCT係数(DCTブロック)の内、隣り合った2つのDCTブロック(ブロック1, 2; 図7(B)等)同士を対応付け、6144個のDCT係数のペア(図7(B), (C))を生成し、データ抽出部428に対して出力する。つまり、対応付部426は、埋込部30(図2, 3)の画像分割部320(図4)に対応し、画像分割部320と同様に、DCTブロックのペアを生成する。

【0120】[乱数発生部420] 乱数発生部420は、鍵情報DB22(図2)から供給され、埋込部30が埋め込みデータの埋め込みに用いた鍵と同じ鍵を用いて、埋込部30においてと同じ方法により乱数RNを発生し、発生した乱数RNを、位置決め部422および抽出順序生成部424に対して出力する。つまり、乱数発生部420は、埋込部30の乱数発生部322(図4)に対応し、乱数発生部322が用いる鍵と同一の鍵から、乱数発生部322と同一方法で同一の乱数を生成する。

【0121】[位置決め部422] 位置決め部422は、乱数発生部420から入力された乱数RNから、ペアそれぞれに含まれる2つのDCTブロック(ブロック1, 2)のいずれのDCT係数が、埋込部30において埋め込みデータの埋め込みに用いられたかを示す位置データを生成し、データ抽出部428に対して出力する。つまり、位置決め部422は、埋込部30の位置決め部324に対応し、位置決め部324が用いた乱数と同一の乱数から、位置決め部324と同一の位置データを生成する。

【0122】[抽出順序生成部424] 上述したように、対応付部426からデータ抽出部428に入力される6144個のペアは、96個のペアを1組として、各組ごとに異なる順番で、各組に含まれる96個のペアそれぞれに、96ビットの埋め込みデータのビットそれぞれが対応付けられている。抽出順序生成部424は、乱数発生部420から入力された乱数RNから、いずれのペアに、96ビットの埋め込みデータのいずれの順番のビットが対応付けられたかを示す順序データを生成し、データ抽出部428に対して出力する。

【0123】データ抽出部428は、対応付部426から入力されるペアそれぞれに含まれる2つのDCTブロック(ブロック1, 2)において、位置決め部422から入力される位置データが示す相互に対応するDCT係

数(図8等)同士の値の関係が、上記表1に示した規則1-1, 1-2のいずれと一致するかを判定し、各ペアに埋め込まれた埋め込みデータのビットの値を抽出する。さらに、データ抽出部428は、抽出したビットの値を、抽出順序生成部424から入力される順序に従って並び替え、図18、19に例示した形式の抽出データを生成し、抽出順序生成部424に対して出力する。

【0124】データ抽出部428のビット抽出処理を、図22を参照してさらに説明する。図22は、図14に示したデータ抽出部428が、各ペアに埋め込まれた埋め込みデータのビットを抽出する処理を示すフローチャートである。図22に示すように、ステップ120(S120)において、データ抽出部428は、6144個のペアを示す変数iに1を代入し、初期設定を行う。

【0125】ステップ122(S122)において、データ抽出部428は、変数iが示す第i番目のペアを抽出対象として取り出す。

【0126】ステップ124(S124)において、データ抽出部428は、取り出した抽出対象のペアに含まれる2つのDCTブロック(ブロック1, 2)において、位置決め部422から入力される位置データが示すDCT係数の関係が、上記表1に示した規則1-1, 1-2のいずれに当てはまるかを判定し、規則1-1に当てはまる場合には、第i番目のペアから値1のビットを抽出し、規則1-2に当てはまる場合には、値0のビットを抽出する。さらに、データ抽出部428は、抽出順序生成部424から入力される順序データに基づいて、抽出したビットの値が、埋め込みデータのいずれのビットに対応するかを判定し、抽出データ(図18, 19)中の判定の結果として得られた位置に、抽出したビットの値(1, 0)を書き込む。

【0127】ステップ126(S126)において、データ抽出部428は、変数iが6144であるか否か、つまり、全てのペアからのビットの抽出が終了したか否かを判断し、終了した場合には処理を終了し、これ以外の場合には変数iを1増やしてS122の処理に進む。

【0128】全てのペアからビットの抽出が完了すると、データ抽出部428は、図18、19に例示した抽出データにおいて、96ビットの埋め込みデータのビットそれぞれに対応して抽出された64個の値の多数決を採り、埋込部30(図2, 3)において埋め込まれた埋め込みデータを推定し、各ペアを輝度成分Yとして符号化部404に対して出力する。

【0129】[符号化部404] 符号化部404(図13)は、復号部400から入力されたクロマ成分Cr, Cbおよび符号化部404から入力された輝度成分Yをハフマン符号化して、JPEGデータを生成し、画像合成部406に対して出力する。

【0130】[改変検出部44] 改変検出部44は、データ抽出部428から入力された抽出データ(図18,

19) から、図20に示した2値画像を生成し、画像合成部406に対して出力する。

【0131】[クラスタリング部46]クラスタリング部46は、改変検出部44から入力された2値画像において、改変等がなされたことが示されている範囲を示すクラスタリング画像(図21)を生成し、画像合成部406に対して出力する。

【0132】[画像合成部406]画像合成部406は、操作入力に応じた制御部26の制御に従って、符号化部404から入力されるJPEGデータを伸長し、図5あるいは図15(C)等に例示した画像を生成し、生成した画像をそのまま表示装置100(図1)に表示する。あるいは、画像合成部406は、改変検出部44から入力された2値画像、あるいは、クラスタリング部46から入力されたクラスタリング画像と、伸長の結果として得られた画像とを合成し、図16あるいは図17に例示した画像を生成し、画像中において改変等がなされた部分を表示装置100に表示する。あるいは、画像合成部406は、改変検出部44から入力された2値画像、あるいは、クラスタリング部46から入力されたクラスタリング画像を、そのまま表示装置100に表示して、画像中のいずれの範囲に改変等がなされたかを示す。

【0133】[画像改変判定装置1の埋め込みデータ埋め込み処理]以下、図23を参照して、画像改変判定装置1による埋め込みデータの埋め込み処理を、全体を通して説明する。図23は、図1に示した画像改変判定装置1による埋め込みデータの埋め込み処理(S20)を示すフローチャートである。

【0134】ステップ200(S200)において、復号部300(図3)は、カメラIF104等を介して供給されるJPEGデータをハフマン復号し、輝度成分Yの12288個のDCT係数(DCTブロック)を、データ埋込部32に対して出力する。画像分割部320は、入力されたDCT係数(DCTブロック; 図7(A))を、6144個のペア(図7(B), (C))に分割して、係数操作部328に対して出力する。乱数発生部322は、鍵情報DB22(図2)から入力される鍵を用いて乱数を発生し、発生した乱数RNを位置決め部324およびスクランブル部326に対して出力する。

【0135】位置決め部324は、乱数発生部322から入力される乱数RNを用いて、埋め込みデータの埋め込みに用いられるDCT係数の位置を示す位置データを生成し、係数操作部328に対して出力する。スクランブル部326は、乱数発生部322から入力される乱数RNを用いて、埋込データ生成部20(図2)から入力される96ビットの埋め込みデータをスクランブル処理し、係数操作部328に対して出力する。

【0136】ステップ12(S12)において、まず、

係数操作部328(図4)は、各ペアにおいて、埋め込みデータを埋め込むための操作の対象となるDCT係数($A_1, A_2, B_1, B_2, C_1, C_2$; 図8等)を、位置決め部324から入力される位置データに基づいて選択する。さらに、係数操作部328は、各ペアを、スクランブル部326から入力される埋め込みデータの各ビットと対応付け、図11に示した埋め込みテーブルを作成する。さらに、係数操作部328は、埋め込みテーブルから操作の対象となるDCT係数と、埋め込むビットとを順次、取り出し、上記表1に示した規則1-1, 1-2に従って、図9(A), (B)および図10に例示したように、各ペアに埋め込みデータの各ビットを埋め込む。

【0137】全てのペアへのビットの埋め込みが終了すると、ステップ202(S202)において、符号化部304(図3)は、埋め込みデータが埋め込まれた輝度成分のDCT係数(DCTブロック)と、復号部300から入力されるその他の成分のDCT係数とをハフマン符号化し、JPEGデータを生成して画像DB22(図2)に対して出力する。画像DB22は、埋込部30から入力されたJPEGデータを記憶・管理する。

【0138】[画像改変判定装置1の埋め込みデータ抽出処理]以下、図24を参照して、画像改変判定装置1による埋め込みデータの抽出処理を、全体を通して説明する。図24は、図1に示した画像改変判定装置1による埋め込みデータの抽出処理(S22)を示すフローチャートである。

【0139】ステップ220(S220)において、復号部400(図13)は、画像DB22から供給されるJPEGデータをハフマン復号し、輝度成分Y'を、画像分割部402に対して出力する。画像分割部402は、輝度成分Y'を12288個のDCT係数(DCTブロック)に分割して、埋込データ抽出部42に対して出力する。埋込データ抽出部42において、対応付部426は、隣り合ったDCT係数(DCTブロック; 図7(A))を2つずつ対応付けて、6144個のペア(図7(B), (C))を作成し、データ抽出部428に対して出力する。乱数発生部420(図14)は、鍵情報DB22(図2)から入力される鍵を用いて乱数を発生し、発生した乱数RNを位置決め部422および抽出順序生成部424に対して出力する。

【0140】位置決め部422は、乱数発生部420から入力される乱数RNを用いて、埋め込みデータの埋め込みに用いられるDCT係数の位置を示す位置データを生成し、データ抽出部428に対して出力する。抽出順序生成部424は、乱数発生部322から入力される乱数RNを用いて、各ペアに、いずれの埋め込みデータのビットが対応付けられているかを示す順序データを生成し、データ抽出部428に対して出力する。

【0141】ステップ12(S12)において、図22

に示したように、データ抽出部428は、ペアを順次、取り出して抽出対象とし、位置決め部422から入力される位置データが示す2つのDCTブロック（ブロック1, 2）のDCT係数の値の関係が、上記表1に示した規則1-1, 1-2のいずれに当てはまるかに応じて、各ペアに埋め込まれたビットの値を抽出する。さらに、データ抽出部428は、抽出順序生成部424から入力される順序データに基づいて、抽出したビットの値が、埋め込みデータのいずれのビットに対応するかを判定し、抽出データ（図18, 19）中の判定の結果として得られた位置に、抽出したビットの値（1, 0）を書き込む。

【0142】全てのペアからのビットの値の抽出が終了すると、ステップ222（S222）において、データ抽出部428は、図18, 19に例示した抽出データにおいて、96ビットの埋め込みデータのビットそれぞれに対応して抽出された64個の値の多数決を採り、埋込部30（図2, 3）において埋め込まれた埋め込みデータを推定する。さらに、符号化部404（図13）は、復号部400から入力されたクロマ成分Cr, Cbおよび符号化部404から入力された輝度成分Yをハフマン符号化して、JPEGデータを生成し、画像合成部406に対して出力する。

【0143】ステップ224（S224）において、改変検出部44は、データ抽出部428から入力された抽出データ（図18, 19）から、図20に示した2値画像を生成し、画像合成部406に対して出力する。クラスタリング部46は、改変検出部44から入力された2値画像において、改変等がなされたことが示されている範囲を示すクラスタリング画像（図21）を生成し、画像合成部406に対して出力する。画像合成部406は、操作入力に応じた制御部26の制御に従って、例えば、改変検出部44から入力された2値画像、あるいは、クラスタリング部46から入力されたクラスタリング画像と、伸長の結果として得られた画像とを合成し、図16あるいは図17に例示した画像を生成し、画像中において改変等がなされた部分を表示装置100に表示する。

【0144】[変形例] 以下、本発明の実施形態の変形例を説明する。

【0145】[画像データの領域] ここまで説明した実施形態においては、画像データの全領域をペアに分割し、画像データの全領域に対して改変の判定を行う場合を具体例としたが、画像データの分割および改変の判定は、画像データの一部の領域に対して行っても、分割した領域と改変を判定する領域とが一致しなくてもよい。

【0146】[DCT以外の変換方式] また、実施形態においては、画像データの圧縮符号化のためにDCT処理を行う場合について説明したが、本発明にかかる改変判定方法は、DCT処理ではなく、例えばウェーブレッ

ト変換、フーリエ変換およびFFT（高速フーリエ変換）といった、空間領域のデータを周波数領域のデータに変換する空間・周波数変換を用いて画像データを圧縮符号化する場合にも、ほとんど変更なしに適用することができる。

【0147】[輝度成分以外への埋め込み] また、実施形態においては、輝度成分YのDCT係数に埋め込みデータを埋め込む場合を説明したが、本発明にかかる改変判定方法は、クロマ成分Cr, Cbに埋込データを埋め込む場合にも応用可能である。また、本発明にかかる改変判定方法は、RGB画像データ等、他の形式の画像データに対して適用できることは言うまでもない。

【0148】[DCTブロックの対応付け] また、実施形態においては、DCTブロックの対応付けを、隣接した2つのDCTブロック同士を対応付けることにより行ったが、例えば、乱数を用いて、12288個のDCTブロックの2つをランダムに選択し、対応付けてペアとしてもよい。また、図4に点線で示したように、乱数発生部322から画像分割部320に乱数RNを供給し、画像分割部320が、この乱数RNを用いて、ランダムに2つずつDCT係数（DCTブロック）を選択してペアを作成するようにしてもよい。

【0149】また、図14に点線で示したように、乱数発生部420から対応付部426に乱数RNを供給し、対応付部426が、この乱数RNを用いて、画像分割部320が対応付けたペアを再現するようにしてもよい。また、埋込データのスクランブル方法は、実施形態として示した方法に限定されず、埋込データの各ビットが、総ペアに対して定数回ずつ割り当てられるような方法であればよい。

【0150】[画像データ以外への適用] また、本発明にかかる埋込・判定プログラム2を適切に変形することにより、画像データの他、音声データ等、他の種類のコンテンツデータのいずれの部分に改変が加えられたかを判定する用途に応用することができる。

【0151】音声データに対して本発明を応用する場合を例としてさらに説明する。音声データは、連続するサンプル点を1ブロックとして処理することができ、例えば、サンプリング周波数44.1kHzの音声データ、1024個ずつを1つのブロックとすれば、1秒分の音声データには、44個の音声データブロックが含まれることになる。これらの音声データブロックをFFTなどにより周波数領域のデータブロックに変換すると、実施形態と同様な方法により埋込データを埋め込むことができ、埋め込んだデータを用いて改変を検出することができる。

【0152】[複数の改変判定装置1の接続方法] 図25は、それぞれ画像DB24（24-1～24-n）を有する複数の画像改変判定装置1（1-1～1-n）を接続した改変判定システム4の構成を示す図である。な

お、図25に示すように、それぞれ画像DB24(24-1~24-n)および埋込・抽出部3(3-1~3-n)を1つつ含む複数の画像改変判定装置1-1~1-nを、通信装置116(図1;図25において図示せず)を介して接続して、各画像改変判定装置1-1~1-nで画像データに加えられた改変を検出する場合に、各画像DB24-1~24-nにおいて記憶・管理される画像データと、その鍵とを、画像改変判定装置1-1の鍵情報DB22-1により一元管理し、各画像改変判定装置1-1~1-nに対して鍵を配送するようにすると、高いセキュリティを確保することができる。

【0153】[コンテンツデータ鑑定装置]次に、上記改変判定装置を用いて、デジタルデバイスにより作成されたコンテンツデータを証拠物件として扱えるようにするための、高度なセキュリティ保持のしくみに取り入れた、コンテンツデータ鑑定装置の実施例を示す。なお以下で使用する、タンパープルーフ(TamperProof)の技術については、機密性の高いアルゴリズムが含まれるソフトウェア/ハードウェア・モジュールを逆アセンブラ等のリバース・エンジニアリングから守るための周知技術である。またRC4とはRon Rivest(RSADataSecurityInc.)が作った暗号化アルゴリズムであり周知技術である。その暗号化のアルゴリズムについての説明は省力する。図26に本発明のデータ鑑定装置のブロック図を示す。デジタルカメラ510で生成されたJPEG画像が、改ざん/すり替え等によりオリジナリティーが毀損されることなくPC上デバイスドライバ・プログラム530(以降単にドライバと呼ぶ)を経て記憶装置(ハードディスクなど)に保存出来る。またPC上のアプリケーション550によりJPEG画像のオリジナリティーを検査し、その結果を表示する。加えて、JPEG画像が改ざんされていた場合は、その改ざん場所も特定することができる。ここで注意すべきは、デジタルカメラ510で生成されたJPEG画像は、510-520間での鍵(Kdc)による認証、520-530間での鍵(Kpc)による認証、530-540間での鍵(Kapp)による認証により(つまり複数の認証を経て)守られていることである。このように高度なセキュリティを保持することにより、デジタルコンテンツの証拠能力を飛躍的に高めることができる。なおドライバ530および電子透かしの埋め込みを行う登録アプリケーション540の動作するPCを、電子透かしを埋め込む装置として実施してもよいし、埋め込まれた電子透かしを抽出し、JPEG画像の改ざん場所を特定するアプリケーション550が動作するPCを、専用の電子透かし抽出装置として実施してもよい。また電子透かしおよびその抽出を同一のPCで行っても何ら構わない。

【0154】図46に本発明で用いるデジタルカメラ510とCF520のハードウェアブロック図を示す。始めにデジタルカメラ510、CF520、ドライバ530

0の間では特定の共通のコマンド(RequestSeedコマンド、SendSeedコマンド)を定義しておく。一般の装置はこれらのコマンドに対して、エラーを返すかタイムアウトになる。RequestSeedコマンドはクライアントにシードを送信するように要求するコマンドであり、SendSeedコマンドはクライアントにこれからシードを送信することを知らせるコマンドである。認証はこれらのコマンドをデバイス間で相互に発信し、要求された数値が返ってくるかどうかで行われる。次にデジタルカメラ510とCF520は共通の鍵Kdcを持っている。該鍵Kdcはデジタルカメラ510のROM領域に記憶されている。またCF520のNAND領域521(Read/Write可能なメモリ領域)にCF520の鍵Kcfにより暗号化されて記憶されている。CF520のNAND領域に記憶する理由は、特定のデジタルカメラで使ったCFを多くのデジタルカメラで利用する場合があるからである。CF520内のKdcは初期化の段階でどのデジタルカメラと一緒に使用されるかの情報として該鍵Kdcを保持する。なお初期化のプロセスを行うことにより、鍵Kdcは変更が可能である。また鍵KcfはCF520を特定するための鍵である。またCF520の記憶領域にはRAM領域525、NAND領域521があるが、RAM領域は主に演算、データの受け渡しなど臨時的に使用され、NAND領域は画像データや鍵情報の保存に主に使用される。CPU522は乱数発生、暗号化(RC4)のための演算、比較などを主に行う。CF520のNAND領域521には鍵Kcfにより暗号化された鍵Kdcのほかに、生の画像データ(JPEG)、分割された画像データから得られる暗号化データ、鍵Kpc、デジタルカメラIDファイル、使用者IDファイル、撮影日、CF520のシリアル番号などが記憶される。NAND領域521の暗号化された鍵、データはRAM領域525のデータと異なり、通常の方法で読み取ってもそのデータは解読不能である。また各鍵データベース560、570、580、590は、予め各デバイスに記憶されるべき鍵情報を有している。この鍵情報を使用して各デバイスは認証を行う。鍵データベース560には、デジカメ使用機器IDと秘密鍵Kdcの組が保存されている。鍵データベース570には、使用者IDと秘密鍵Kpcの組が保存されている。これらのデータベースはCF520の初期化の時に使用される。CF520はデジタルカメラの内部にセットされる前に以下の手順で初期化される。

(1) 使用者IDをCF520内のRAM領域525に保存する。

(2) 鍵KpcをCF520内のNAND領域521に保存する。

(3) 使用機器IDファイルをCF520内のNAND領域525に保存する。

(4) 鍵KdcをCF520内のNAND領域521に保

存する。

CF520のNAND領域に保存されている鍵Kdc、Kpcは各デバイスとの認証に使用する数列作成に用いられる。このように初期化されたCF520とデジタルカメラは次のようにして認証とデータの保存を行う。まずデジタルカメラ510の認証部513とCF520の認証部523は共通の鍵Kdcを用いた認証を行う。認証成功に伴い、デジタルカメラ510は、CCDなどのデバイスからなる画像取り込み部511にて画像信号を発生させ画像処理部512に送られ画像データとなる、この画像データがCF520のNAND領域521に書き込まれる。ただしこのとき平行してその画像データは随時512バイトづつ、鍵KcfおよびCF520のシリアル番号により暗号化されてNAND領域521に暗号データとして書き込まれる。好適にはROM領域523をタンパブルーフにしておく。以降CF520内に画像を保存するという場合、NAND領域521に画像データそのものが記憶され、さらにNAND領域521には分割画像データから得られる暗号化されたデータが保存されることを意味数する。

【0155】図31にデータ鑑定方法のメイン・フローチャートを示す。ステップS1000はJPEG画像生成を行うステップである。デジタルカメラ510でJPEG画像を生成し、S2000の、510-520間認証に渡す。ステップS2000は、510-520間認証を行うステップである。デジタルカメラ510とCF520間で認証を取り合い、その結果とJPEG画像をCFに保存する。ステップS3000は、520-530間認証を行うステップである。CF520とCF用ドライバ530間で認証を取り合い、その結果をS4000の530-540間認証に渡す。ステップS4000は、530-540間認証を行う。CF用ドライバ530とJPEG画像登録・保存アプリケーション540間で認証を取り合い、その結果をS5000の540-550間認証に渡す。ステップS5000はID等埋め込みを行うステップである。S2000の510-520間認証、S3000の520-530間認証、S4000の530-540間認証の結果を表示し、JPEG画像にID、改ざん有無検出用マークを埋め込む。ステップS6000はID等抽出／検出を行うステップである。JPEG画像に埋め込まれたIDを抽出、改ざん有無検出用マークを検出し、その結果を表示する。また改ざんがあった場合は改ざん場所をJPEG画像とともに表示する。

【0156】次にステップS2000の510-520間認証のフローチャートを図32に示す。ステップS2100は510-520間認証判定を行うステップである。510-520間の認証用鍵(Kdc)によりデジタルカメラ510とCF520間の認証をした後、S1000のJPEG画像生成により生成されたJPEG画像と認証結果を出力する。ステップS2200はCF520へのJP

EG保存を行うステップである。S2100の判定結果とJPEG画像をCF520内JPEG画像保存用鍵(Kcf)を用いて、CF520内にJPEG画像を保存する。

【0157】次にステップS2100の510-520間認証判定の詳細フローチャートを図33に示す。まずS2100でCF520が乱数の数列(a)を生成する。そしてCF520はこの生成した数列(a)をデジタルカメラ510へ送る。ステップS2120でデジタルカメラ510は受け取った数列(a)をデジタルカメラ510内部に持つ鍵Kdcを用いて暗号化する。そしてその暗号化の出力である数列(b)を生成する。ここでCF520はステップS2130で独自に乱数(a)からCF内部に持つ鍵Kdcを入力としてRC4の暗号化(演算は図46のCF520内のCPU522により行われる)を行い、その出力である数列(c)を生成する。そしてステップS2140で、CF520は、デジタルカメラ510で計算された送られた数列(b)と内部で作成した数列(c)を比較する。その比較の結果、同じだった場合はデジタルカメラ510とCF520が持つ鍵Kdcは共通のものであるから、デジタルカメラとCFの認証は成功、違っていた場合は、デジタルカメラとCF520の認証は失敗としてS2100の判定結果を得る。

【0158】次にステップS2200のCF520への保存の詳細フローチャートを図34に示す。デジタルカメラ510とCF520間の認証が成功した場合、次にデジタルカメラ510で生成された画像をCF520内にKcfを用いて保存する。ステップS2210はJPEG画像分割を行うステップである。デジタルカメラ510で生成されたJPEG画像を512byteづつに分割する。ステップS2220は510-520間認証判定を行うステップである。S2100の510-520間認証判定の出力結果である2100判定結果から、デジタルカメラ510とCF520間の認証が失敗している場合は、CF内のNAND領域に0の数列を書き込み、認証が成功している場合、ステップS2230でデジタルカメラ510で生成された画像をCF520内の鍵Kcfを用いてNAND領域521に記憶する。この時鍵KcfはCF520のROM領域523に保存されている。S2210の出力結果である512byteのデータとCF520のシリアル番号、CF520内に内蔵されている該鍵Kcfを用いてRC4による計算を行い、その結果の数列をCF520内のNAND領域521に書き込む。

【0159】次にステップS3000の520-530間認証のフローチャートを図35に示す。ステップS3100は520-530間認証判定を行うステップである。520-530間の認証用鍵(Kpc)によりCF520とCFドライバ530間の認証をした後、認証結果S3100を出力する。

【0160】次にステップS3100の520-530間認証判定の詳細フローチャートを図36に示す。まず

鍵データベース570の中には予めCF520のユーザーIDと鍵Kpcがペアとなって保存されている。またCF520内には、ユーザーID、鍵KpcがNAND領域521に保存されている。ステップS3110は520-530間認証用乱数生成を行うステップである。CFドライバ530が認証のために使用する乱数(a)を生成する。ステップS3120はCF520において認証用数列を生成するステップである。CF520内のNAND領域521にあらかじめ入っている鍵Kpcと、S3110の出力結果である乱数(a)を使って、RC4によって計算される数列(b)を出力する。ステップS3130はCFドライバ530側の認証用数列生成を行うステップである。CFドライバ530は鍵Kpcと、S3110の出力結果である乱数(a)を使って、RC4によって計算される数列(c)を出力する。ステップS3140は520-530間認証用数列判定を行うステップである。CFドライバ530がS3120の出力結果である数列(b)とS3130の出力結果である数列(c)を比較し、両者が同じ物であった場合「CFとCFドライバ間の認証は成功」という結果を出力する。両者が違う物であった場合「CFとCFドライバ間の認証は失敗」という結果を出力する。好適には、認証失敗の場合、これ以降の認証の処理を行わないで、アプリケーション540上でCF520内の画像が表示される時、「コンパクトフラッシュドライバとコンパクトフラッシュ間の認証に失敗しているため、オリジナリティーが確認できない画像です」という警告メッセージを表示装置100に表示する。

【0161】次にステップS4000の530-540間認証のフローチャートを図37に示す。ステップS4100は530-540間認証判定を行うステップである。530-540間の認証用鍵(Kapp)によりCFドライバ530とJPEG画像登録・保存アプリケーション540間の認証をした後、認証結果S4100を出力する。

【0162】次にステップS4100の530-540間認証の詳細フローチャートを図40に示す。このステップS4110ではまずアプリケーション540が認証のために使用する乱数(a)を生成する。ステップS4120はCFドライバ530が認証用数列(b)を生成するステップである。CFドライバ530は鍵Kappと、S4110の出力結果である乱数(a)を使って、RC4によって計算される数列(b)を出力する。ステップS4130はアプリケーション540が認証用数列(c)を生成するステップである。アプリケーション540は、アプリケーション540内にあらかじめ入っている鍵Kappと、S4110の出力結果である乱数(a)を使って、RC4によって計算される数列(c)を出力する。ステップS4140は530-540間認証用数列判定を行うステップである。S4120の出力結果で

ある数列(b)とS4130の出力結果である数列(c)を比較し、両者が同じ物であった場合「CFドライバとアプリケーション間の認証は成功」という結果を出力する。両者が違う物であった場合「CFドライバとアプリケーション間の認証は失敗」という結果を出力する。好適には、認証が失敗した場合、これ以降の認証の処理を行わないで、アプリケーション540上でCF520内の画像が表示される時、「アプリケーションとコンパクトフラッシュ・ドライバ間認証に失敗しているため、オリジナリティーが確認できない画像です」という警告メッセージを表示装置100に表示する。使用者によりデータベースに登録するために選ばれた画像が「オリジナリティーが確認できない画像」だった場合は、画像に電子透かしにより埋め込まれる情報の中に「登録する前にオリジナリティーが確認されなかった画像」(すなわち出所が確認されなかった画像)という情報を含ませる。

【0163】次にステップS5000のID埋め込みのフローチャートを図38に示す。ステップS5100はCF520内のJPEG検査を行うステップである。CF520内に保存されているJPEG画像に改ざんが行われたかどうかを検査する。ステップS5200はID埋め込みを行うステップである。データ埋め込み/抽出用鍵(Kdh)を用いて、イメージID(ID情報)をJPEG画像に電子透かしにより埋め込む。

【0164】次にステップS5100のCF520内JPEG検査の詳細フローチャートを図39に示す。ステップS5110はCF520内JPEG画像分割を行うステップである。CF520内に保存されているJPEG画像を512byteづつに分割する。ステップS5120はデータ判定用数列生成を行うステップである。アプリケーション540はS5110の出力結果である512byteのデータとCF520のNAND領域521に記憶されているシリアル番号、CF520内のROM領域523に内蔵されている鍵Kcfを用いてRC4を行い、その結果の数列(a)を出力する。ステップS5130はデータ判定用数列読取りを行うステップである。CF520内のNAND領域521に書かれている数列(b)を出力する。ステップS5140はデータ判定用数列比較を行うステップである。S5120の出力結果である数列(a)とS5130の出力結果である数列(b)を比較し、両者が同じ物であった場合「512byteのデータは改ざんがされていない」という結果を出力し、分割された次のデータへ処理を進める。両者が違う物であった場合「512byteのデータは改ざんがされているので、このJPEGデータは改ざんされている」という結果を判定結果S5100として出力する。

【0165】次にステップS5200のID埋め込みの詳細フローチャートを図41に示す。ステップS5210はイメージID生成を行うステップである。JPEG画像に電

子透かしによって埋め込むデータ（イメージID）を生成する。イメージIDは判定結果S3100、判定結果S4100、判定結果S5100による認証履歴情報、撮影日、撮影者（使用者ID）、登録日、撮影機器（デジタルカメラID）などから生成される数値である。ここでいう認証履歴情報とはデジタルカメラ510から、JPEG画像登録・保存アプリケーション540の間の認証はすべて成功しているか、あるいは失敗しているかという情報、CF520内JPEG画像の改ざんの有無をあらわす情報などを含む、いわゆる過去の認証の履歴を表わす情報である。後程この認証履歴情報を抽出することによりどの時点で認証ができなくなったか（どの過程で改竄された可能性があるか）が分る。ステップS5220はイメージID埋め込みを行うステップである。データ埋め込み／抽出用鍵（Kdh）を用いて、イメージIDをJPEG画像に電子透かしにより埋め込み電子透かしが施されたJPEG画像を出力する。

【0166】次にステップS6000のID等抽出／検出の詳細フローチャートを図42に示す。ステップS6100はID抽出を行うステップである。データ埋め込み／抽出用鍵（Kdh）を用いて、イメージIDをJPEG画像から電子透かしにより抽出する。ステップS6200は抽出検出結果解析表示を行うステップである。S6100（ID抽出）で抽出したID、改ざんの有り無し、（改ざんがあった場合）改ざん場所をJPEG画像とともに表示する。

【0167】次にステップS6100のID抽出のより詳細なフローチャートを図43に示す。ステップS6110はイメージID抽出を行うステップである。JPEG画像から電子透かしによって埋め込まれたデータ（イメージID）をデータ埋め込み／抽出用鍵（Kdh）を用いて抽出する。ステップS6120はイメージID解析 改ざん有無判定を行うステップである。S6110の出力結果から認証履歴情報、撮影日、撮影者、登録日、撮影機器などを解析し、さらに画像中に改ざんされている場所があるかどうかを電子透かしを用いて検査する。その結果、改ざん場所が観測された場合は、S6130（改ざん場所特定）処理に移り、改ざん場所がなかった場合は、解析した結果（認証履歴情報、撮影日、撮影者、登録日、撮影機器など）をS6100検出結果として出力する。ステップS6130は改ざん場所特定を行うステップである。S6120の結果が改ざんあり、と判定された場合、改ざん場所特定処理を行い、改ざん場所を二値画像化し、S6120の解析した結果（認証履歴情報、撮影日、撮影者、登録日、撮影機器など）とともにS6100検出結果として出力する。

【0168】[保険業務] 図44に、本発明のデータ鑑定装置を用いたクレームサービス、損害査定業務の概要を示す。本発明は、保険の掛けられた対象に損害を生じ、契約者から保険会社に損害保険の支払い請求があつ

た場合に、保険会社が調査に基づいて損害額を査定し保険金の支払いを行う、損害査定業務などにそのまま適用できる。本発明のデータ鑑定装置を用いることにより損害対象の証拠デジタル写真が改ざんやすり替え等から守られ、損害査定業務を安全かつ効率的に行う事ができる。なお同様に、損害保険業務に関わらず、証拠書類として対象物や現場の写真を用いる土木・建築業務、官公庁の不動産管理、環境開発・保全、災害対策などの広汎な業務に適用できる。図44の損害査定業務の概要を自動車保険のケースに適用して説明する。保険を契約している顧客またはその代理店640から事故の報告を受けた保険会社660は、ただちにその事故を担当する保険会社支社650に通報する。保険会社の支社マネージャは、査定員630を指名し、損害調査の指示をする。査定員630は損害車両が保管されている修理工場などに赴き車両を調査し、デジタルカメラを用いて損害の証拠のため写真撮影を行い、損害額の査定を行う。また査定員630はPCを用いてこの事故案件についての詳細／証拠写真ファイルが添付された査定書を作成する。そして査定員630は査定書を、支店マネージャの承認を受けるために提出／事故案件データベース600に登録する。支店マネージャは査定員の提出した事故案件を鑑定／承認し、保険金の支払いが行われる。

【0169】[保険業務プロセス] 次に、本発明の方法が組み込まれた損害査定業務プロセスの流れを図45に示す。まず査定員630がデジタルカメラ510で撮った写真が、デジタルカメラ内でJPEG画像として生成される。次に生成されたJPEG画像はデジタルカメラ510内に入れられているコンパクトフラッシュ520に相互認証の後、各々保存される。査定員630は、CF520内のJPEG画像を損害査定業務アプリケーション内に登録するために、CF520内に保存されているすべてのJPEGを一覧表示から、登録写真として選択する。損害査定業務アプリケーション540はJPEG写真の一覧表示時、CF520とCF用ドライバ530の相互認証、CF用ドライバ530と損害査定業務アプリケーション540の相互認証を行い、かつ、デジタルカメラ510とCF520の相互認証の結果、CF520内に保存されているすべてのJPEGに対して、入力の正当性を検査し、その結果を表示する。査定員630は、その結果を参照しつつ、事故案件として登録すべき写真を選択する。これにより、信頼のおけるJPEG画像かそうでないか確認できる。認証の結果が無いもしくは認証に失敗した情報を有する写真は、別に撮影された写真画像がPCで改ざんされた後、このCF520に書き込まれた可能性を否定できないので、以下の業務で使用しないと決めれば、この不正行為を未然に防ぐことができる。次に査定員630によって選択されたJPEG写真が事故案件データベース600に保存される。この時、保存されるJPEG写真に、電子透かしにより改ざん有無検出用マークと、撮影日・登

録日・撮影者・認証履歴情報・使用機器等により作られるイメージIDが埋め込まれる。そして損害査定業務アプリケーション540内に登録されているJPEG写真を保険会社マネージャが鑑定する。この時、事故案件データベース600に登録されているJPEG写真は、電子透かしにより改ざん有無の検出と、イメージIDの抽出が行われ、その結果が損害査定業務アプリケーション上に表示される。また、JPEG写真がアプリケーション登録後に改ざんされた場合、その改ざん場所も表示する。なお、改ざん有無の検出を行うPCは、埋め込みと同一のPCでも構わないし、通信で結ばれた遠隔PC610でも構わない。

【0170】本発明は、本人証明を行うシステムに容易に応用できる。図47に本発明をスマートカードに応用した例を示す。スマートカード700には表面に、その所有者の名前、ID番号などが記載されている。好適には本人の写真イメージなどが印刷されている。本スマートカードの特徴的な所は、このような本人を証明するデータをスマートカード内のメモリ領域に電子透かしと埋め込まれている点にある。この電子透かしには、本発明の改変箇所特定を行う改変検出用データを有しているので、改ざん及び改ざん箇所の特定が行える点にある。本人証明を行う証明データ検出方法は、該スマートカード700をスマートカード・リーダー710に読み込ませ、改変検出用データが埋め込まれた所有者の証明データをスマートカードから読み取り、改変検出用データの抽出結果に基づき、前記証明データ改変の有無の判断を行い、改変がなされたと判断した場合に改変箇所の特定を行う。なお、本人証明データとは、その人物の書誌的なデータのほか生物学的特徴である、指紋、声紋、虹彩、網膜などの電子化されたデータをスマートカード700に本発明の改変検出用データを有する電子透かしで記憶しておき、これをスマートカード・リーダー710で読み取り、改変を検知するようにする。改変があった場合にはどこに改変があったかを指摘する。好適には、改ざんがないと判定した後、スマートカード・リーダーで読み取った情報を、窓口に来た人物から得られる情報と比較することにより、最終的な本人証明を終了する。

【0171】[コンテンツデータ鑑定装置の変形例]以下、本発明のデータ鑑定装置のその他の変形例を示す。図27に図26をよりシンプル(PCに付属品としてデジタルカメラ510が接続される)にしたデータ鑑定装置を図示する。登録アプリケーション540でJPEG画像は鍵(Kdh)によるJPEGのID埋め込み(電子透かし)を施された後、ハードディスク上に保存される。表示アプリケーション550は登録アプリケーション540で埋め込まれたIDをJPEG画像から抽出し、また改ざんがあるかどうかを検査し、その結果を表示する。もし改ざんが合った場合は、改ざん場所も検出し表示する。

【0172】図28に、図26におけるデジタルカメラ

510上で電子透かしを施すケースを示す。デジタルカメラ510で生成されたJPEG画像は、鍵(Kdh)によるJPEGのID埋め込み(電子透かし)を施される。メディア520に保存されたJPEG画像は、ドライバ530を経て、PC上の登録アプリケーション540によりハードディスク上に保存される。表示アプリケーション550はデジタルカメラ510で埋め込まれたIDをJPEG画像から抽出し、また改ざんの有無を検査し、その結果を表示する。もし改ざんが合った場合は、改ざん場所も検出し表示する。上記の認証、電子透かしは鍵によって守られているが、これらをタンパプルーフによって守ることにより、機密性がさらに高まる。

【0173】図29に、図26にのデジタルカメラ510からPCへケーブルにより直接接続したケースを示す。デジタルカメラ510で生成されたJPEG画像は、510-530間での鍵(Kpc)による認証と、530-540間での鍵(Kapp)による認証によって守られる。登録アプリケーション540でJPEG画像は、鍵(Kdh)によるJPEGのID埋め込み(電子透かし)を施された後、ハードディスク上に保存される。表示アプリケーション550は登録アプリケーション540で埋め込まれたIDをJPEG画像から抽出し、また改ざんの有無を検査し、その結果を表示する。もし改ざんが合った場合は、改ざん場所も検出し表示する。上記の認証、電子透かしは鍵によって守られているが、これらをタンパプルーフによって守ることにより、機密性がさらに高まる。

【0174】図30に、より柔軟性のあるデータ鑑定装置を示す。デジタルカメラ510で生成されたJPEG画像は、510-520間での鍵(Kdc)による認証と、520-530間での鍵(Kpc)による認証と、530-540間での鍵(Kapp)による認証とによって守られる。登録アプリケーション540でJPEG画像は、鍵(Kdh)によるJPEGのID埋め込み(電子透かし)、鍵(Kalt)による改ざん有無検出用マークの埋め込み(電子透かし)を施された後、ハードディスク上に保存される。表示アプリケーション550は登録アプリケーション540で埋め込まれたIDをJPEG画像から抽出し、また改ざんがあるかどうかを検査し、その結果を表示する。もし、改ざんがあった場合は、改ざん場所も検出し表示する。ここで注目すべきは、JPEG画像データそのものから得られるハッシュ値により計算された鍵(Kalt)のJPEGへのID埋め込みである。埋め込まれた鍵(Kalt)の値と、JPEG画像データから計算されるハッシュ値を比較することで、画像データに改ざんがあるかどうかの判断は瞬時に計算される。この鍵(Kalt)により、改変の有無の判断のみを高速に行うことで改ざんがない場合の処理が高速化される。ただし改ざんがある場合には他のケースと同様に鍵(Kdh)により改ざん場所の特定が行われる。上記の認証、電子透かしは鍵によって守られているが、これらをタンパプルーフによって守ることによ

り、さらに機密性が高まる。

【0175】

【発明の効果】以上説明したように、本発明にかかるデータ鑑定装置およびその方法によれば、コンテンツデータの作成から改変判定までの間に関わる複数の装置間で、適切な認証を行うことにより、単にコンテンツデータの改変および改変箇所の特定制が行えるだけでなく、そのコンテンツデータに対する信頼性を非常に高くすることが可能になる。すなわち、デジタルカメラやデジタル録音装置などのデジタルデバイスを用いて作成された画像データ、音声データを証拠物件として扱えるようにするための、高度なセキュリティ保持のしくみが提供される。

【図面の簡単な説明】

【図1】本発明にかかる改変判定方法を実現する画像改変判定装置の構成を示す図である。

【図2】図1に示した画像改変判定装置が実行し、本発明にかかる改変判定方法を実現する埋込・判定プログラムの構成を示す図である。

【図3】図2に示した埋込部30の構成を示す図である。

【図4】図3に示したデータ埋込部32の構成を示す図である。

【図5】デジタルカメラ（図1）が撮影した非圧縮画像データを例示する図である。

【図6】（A）は、図5に例示した非圧縮画像データの一部を示す図であり、（B）は、（A）に例示した非圧縮画像データ（部分）に含まれるDCTブロック（マクロブロック）を示す図であり、（C）は、（B）に示したDCTブロックそれぞれに含まれる8画素×8画素構成の画素を示す図である。

【図7】（A）は、デジタルカメラから入力される圧縮画像データを復号部がハフマン復号して得られる輝度信号YのDCT係数を示す図であり、（B）は、（A）に示した輝度信号YのDCT係数の内、それぞれ隣り合う2組を対応付ける方法を示す図であり、（C）は、（B）に示した方法により対応付けられたDCT係数のペアを示す図である。

【図8】図2、3に示した埋込部が1つのペア（図7（A）、（B））に含まれるDCTブロック（ブロック1、2）それぞれから選択した相互に対応するDCT係数を例示する図である。

【図9】（A）、（B）は、図8に例示したように選択されたブロック1、2それぞれのDCT係数を、埋め込みデータのビット（値1）を埋め込むために、DCT係数の数値を変更する必要がある場合について例示する図である。

【図10】図8に例示したように選択されたブロック1、2それぞれのDCT係数を、埋め込みデータのビット（値1）を埋め込むために、DCT係数の数値を変更

する必要がない場合について例示する図である。

【図11】埋込部（図2、3）が、DCTブロックに対して埋め込みデータを埋め込むために用いられる埋め込みテーブルを例示する図表である。

【図12】図4に示した係数操作部が、DCTブロックのペアに埋め込みデータを埋め込む処理（S10）を示す図である。

【図13】図2に示した抽出部の構成を示す図である。

【図14】図13に示した埋め込みデータ抽出部の構成を示す図である。

【図15】（A）は、埋込部（図2、3）が埋め込みデータを埋め込んだJPEGデータを伸長した画像を例示する図であり、（B）は、（A）に示した画像に加えられた改変を例示する図であり、（C）は、改変後の画像を例示する図である。

【図16】改変が加えられた部分を示す2値画像を、元の画像と合成して示す画像を例示する図である。

【図17】クラスタリング処理により、改変が加えられた範囲を示す画像を、元の画像と合成して示す画像を例示する図である。

【図18】埋込部（図2、3）が生成したJPEGデータに、改変・誤りが加えられていない場合に、抽出部が改変等がなされていないJPEGデータに含まれる各ペアから抽出するビットの値を示す図である。

【図19】埋込部（図2、3）が生成したJPEGデータに、改変・誤りが加えられた場合に、抽出部が改変等がなされたJPEGデータに含まれる各ペアから抽出するビットの値を示す図である。

【図20】抽出部（図13、14）が、図15に例示したように改変が加えられたJPEGデータから、図19に例示したように改変等が加えられたペアを判定し、改変が加えられたペアの画像内における位置を示す2値画像を例示する図である。

【図21】（A）～（D）は、抽出部（図13、14）が、図15に例示したように改変が加えられたJPEGデータから、図19に例示したように改変等が加えられたペアを判定し、改変が加えられたペアが画像内において、いずれの範囲に存在するかを示すクラスタリング画像を例示する図である。

【図22】図14に示したデータ抽出部が、各ペアに埋め込まれた埋め込みデータのビットを抽出する処理を示すフローチャートである。

【図23】図1に示した画像改変判定装置による埋め込みデータの埋め込み処理（S20）を示すフローチャートである。

【図24】図1に示した画像改変判定装置による埋め込みデータの抽出処理（S22）を示すフローチャートである。

【図25】それぞれ画像DBを有する複数の画像改変判定装置を接続した改変判定システムの構成を示す図であ

る。

【図26】データ鑑定装置のブロック図である。

【図27】PCに付属品としてデジタルカメラ510が接続されるデータ鑑定装置である。

【図28】デジタルカメラ510上で電子透かしを施すケースを示す図である。

【図29】デジタルカメラ510からPCへケーブルにより直接接続したケースを示す図である。

【図30】より柔軟性のあるデータ鑑定装置を示す図である。

【図31】データ鑑定方法のメイン・フローチャートである。

【図32】ステップS2000の510-520間認証のフローチャートである。

【図33】ステップS2100の510-520間認証判定の詳細フローチャートである。

【図34】ステップS2200のCF520への保存の詳細フローチャートである。

【図35】ステップS3000の520-530間認証のフローチャートである。

【図36】ステップS3100の520-530間認証判定の詳細フローチャートである。

【図37】ステップS4000の530-540間認証のフローチャートである。

【図38】ステップS5000のID等埋め込みのフローチャートである。

【図39】ステップS5100のCF520内JPEG検査の詳細フローチャートである。

【図40】ステップS4100の530-540間認証の詳細フローチャートである。

【図41】ステップS5200のID埋め込みの詳細フローチャートである。

【図42】ステップS6000のID等抽出／検出のフローチャートである。

【図43】ステップS6100のID抽出のより詳細なフローチャートである。

【図44】本発明のデータ鑑定装置を用いたクレームサービス、損害査定業務の概要を示す図である。

【図45】本発明の方法が組み込まれた損害査定業務プロセスの流れを示す図である。

【図46】本発明のデジタルカメラ510およびCF520のハードウェアブロック図である。

【図47】本発明のスマートカードおよびスマートカード・リーダーの概観図である。

【符号の説明】

1, 1-1~1-n・・・画像改変判定装置

100・・・表示装置

102・・・入力装置

104・・・カメラIF

106・・・メモリカードIF

108・・・記憶装置

110・・・PC本体

112・・・メモリ

114・・・CPU

116・・・通信装置

120・・・記録媒体

140・・・デジタルカメラ

142・・・メモリカード

2・・・埋込・判定プログラム

3, 3-1~3-n・・・埋込・抽出部

20・・・埋込データ生成部

22, 22-1・・・鍵情報DB

24, 24-1~24-n・・・画像DB

26・・・制御部

30・・・埋込部

300・・・復号部

32・・・データ埋込部

320・・・画像分割部

322・・・乱数発生部

324・・・位置決め部

326・・・スクランブル部

328・・・係数操作部

304・・・符号化部

40・・・抽出部

400・・・復号部

402・・・画像分割部

404・・・符号化部

406・・・画像合成部

42・・・埋込データ抽出部

420・・・乱数発生部

422・・・位置決め部

424・・・抽出順序生成部

426・・・対応付部

428・・・データ抽出部

44・・・改変検出部

46・・・クラスタリング部

50・・・OS

510・・・デジタルカメラ

511・・・画像取り込み部

512・・・画像処理部

513・・・デジタルカメラ認証部

520・・・コンパクトフラッシュ(CF)

521・・・NAND領域

522・・・CFのCPU

523・・・ROM領域

524・・・CF認証部

525・・・RAM領域

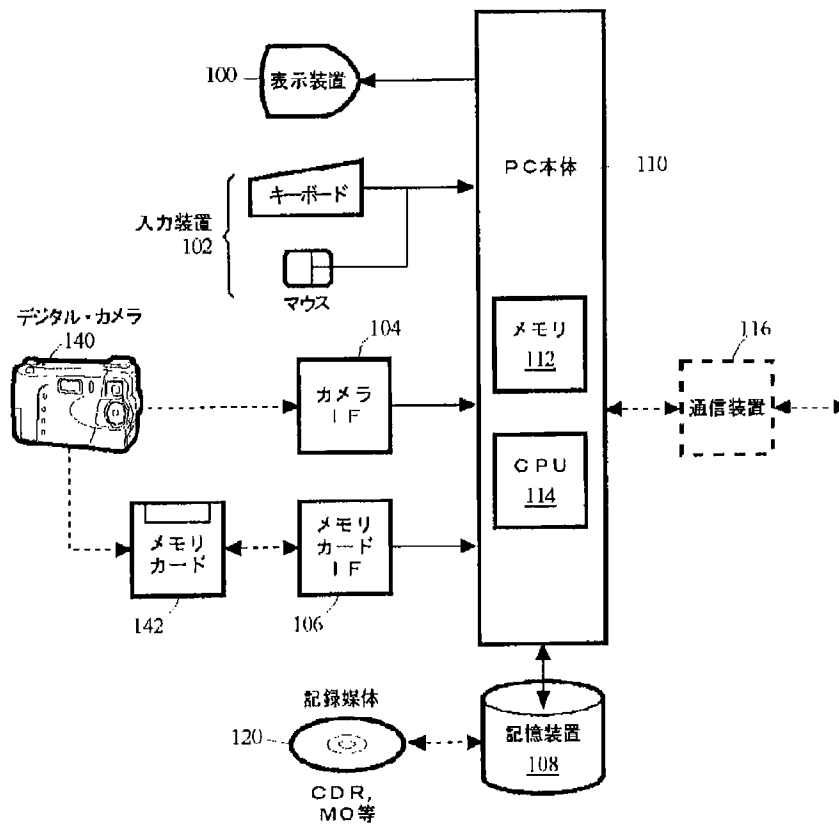
530・・・コンパクトフラッシュ(520)用ドライバ・プログラム

540・・・JPEG画像登録・保存アプリケーション

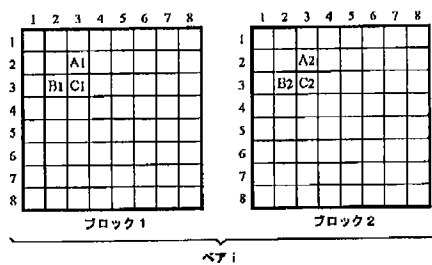
550・・・JPEG画像表示・埋め込みデータ検出/抽出
・改ざん場所検出アプリケーション
560・・・Kdc (510-520間の認証用鍵) のあ
るデータベース
570・・・Kpc (520-530間の認証用鍵) のあ
るデータベース
580・・・Kapp (530-540間の認証用鍵) のあ
るデータベース
590・・・Kdh (データ埋め込み/抽出用鍵) のある
データベース

600・・・事故案件データベース
610・・・埋め込みデータ検出/抽出・改ざん場所検
出用PC
630・・・査定員
640・・・顧客/代理店
650・・・保険会社(支社)
660・・・保険会社(別の支社)
700・・・スマートカード
710・・・スマートカード・リーダー

【図1】

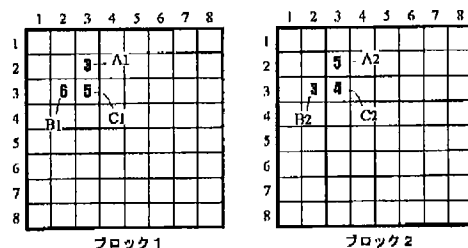


【図8】

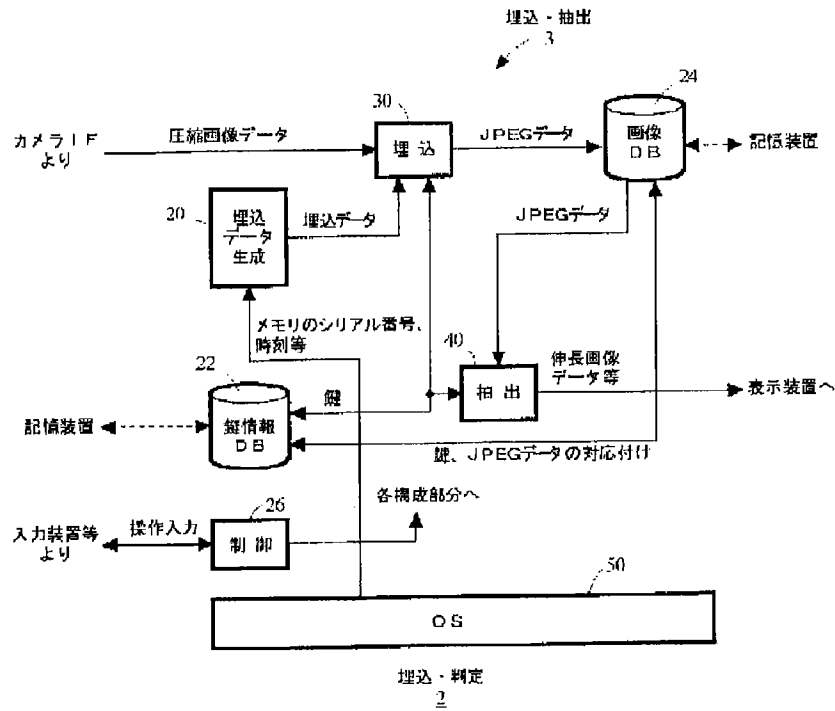


【図10】

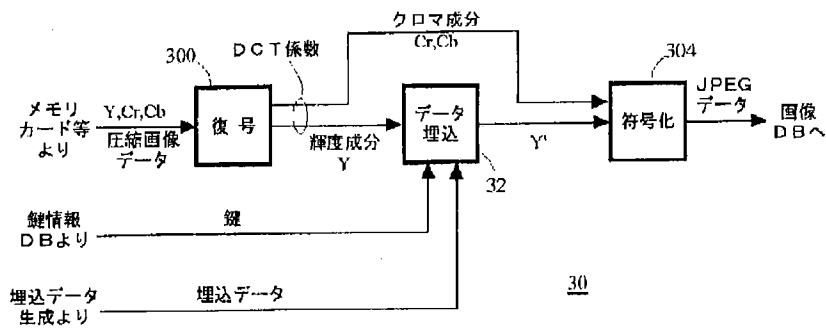
ペア i ← ビット "1" を埋込む



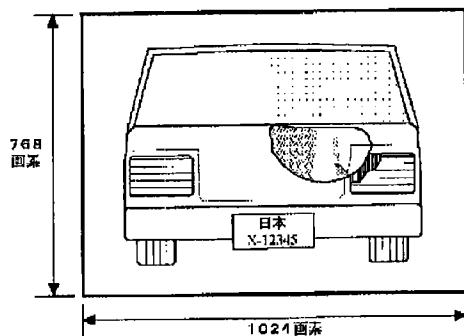
【図2】



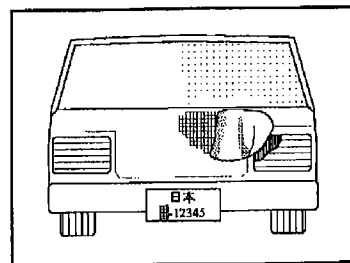
【図3】



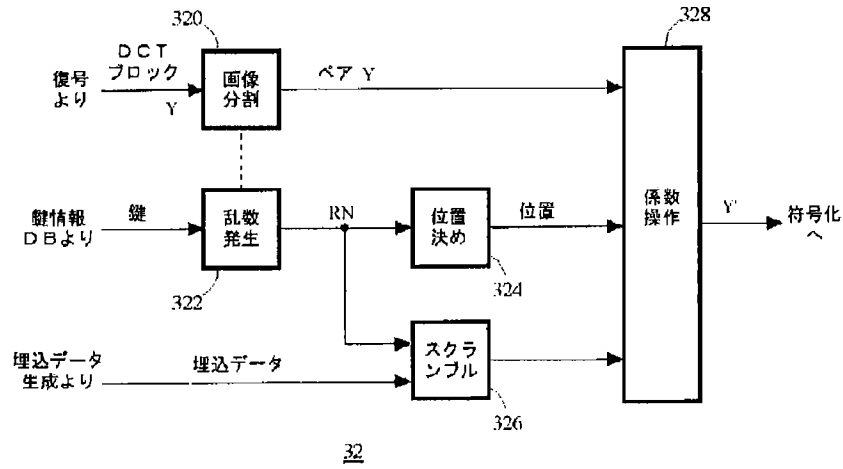
【図5】



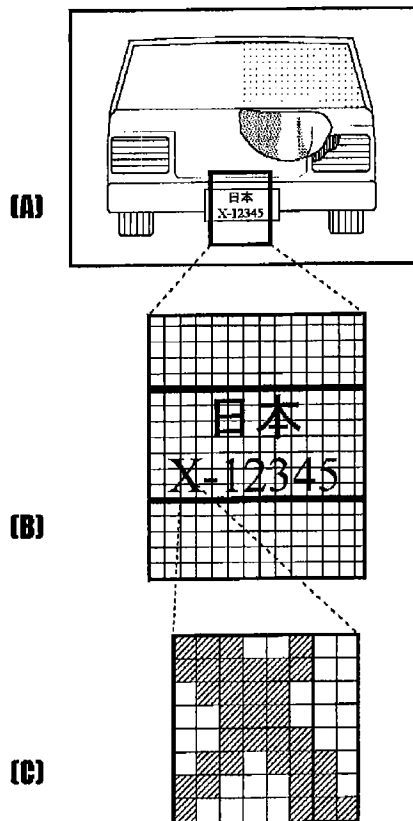
【図16】



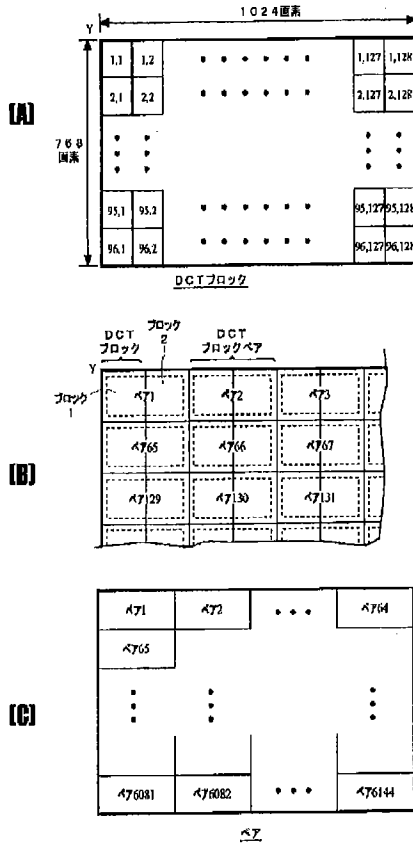
【図4】



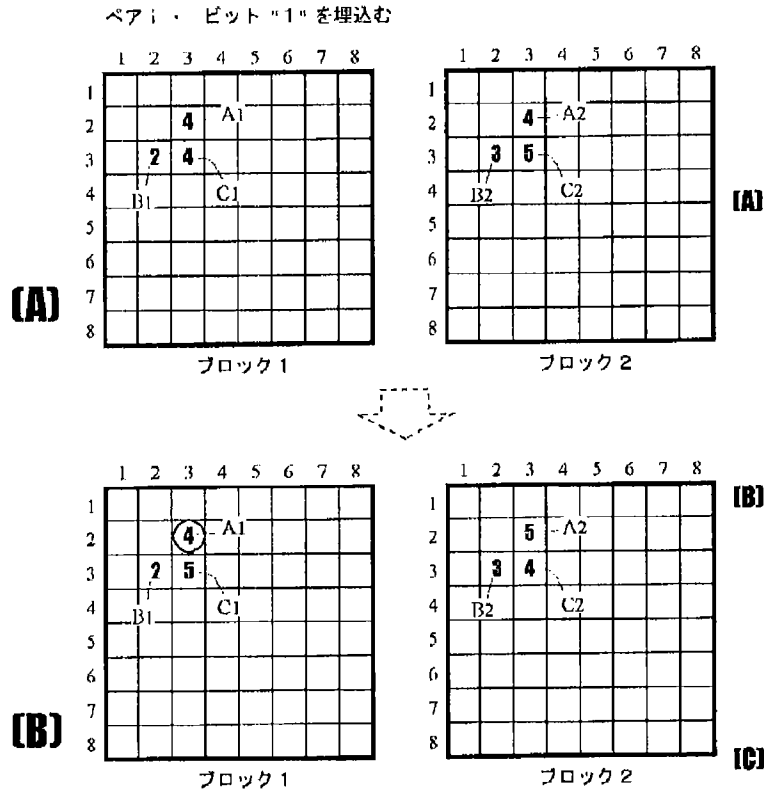
【図6】



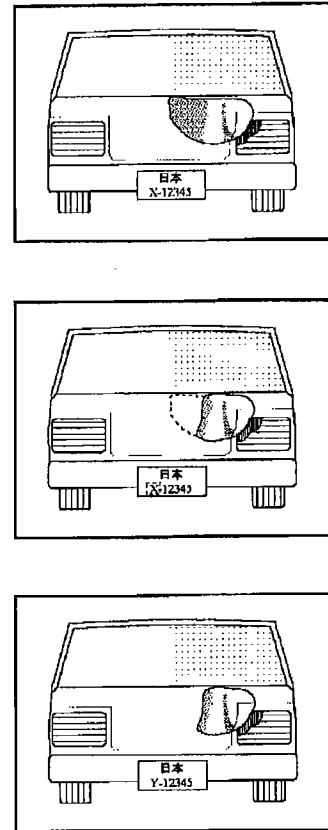
【図7】



【図9】



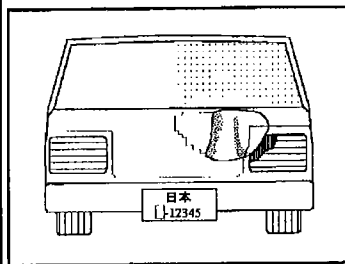
【図15】



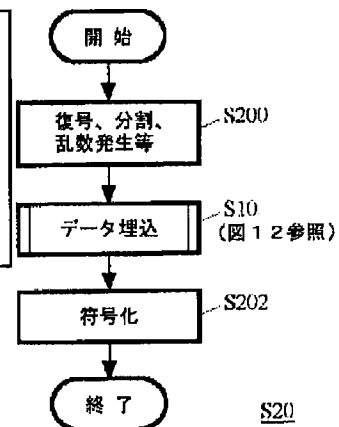
【図11】

DCTブロック ペア番号	ブロック 1 係数			ブロック 2 係数			埋込データ ビット番号	埋込データ 割当て
	A1	B1	C1	A2	B2	C2	(1~96)	
1	1	5	2	5	6	3	31	1
2	5	8	9	2	5	5	21	0
3	2	10	9	5	1	2	18	1
4	1	11	5	5	3	20	65	0
5	10	2	25	1	3	24	7	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
160	5	30	11	6	9	10	7	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
6144	51	20	11	3	19	15	34	1

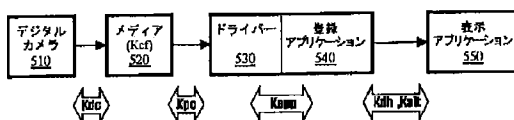
【図17】



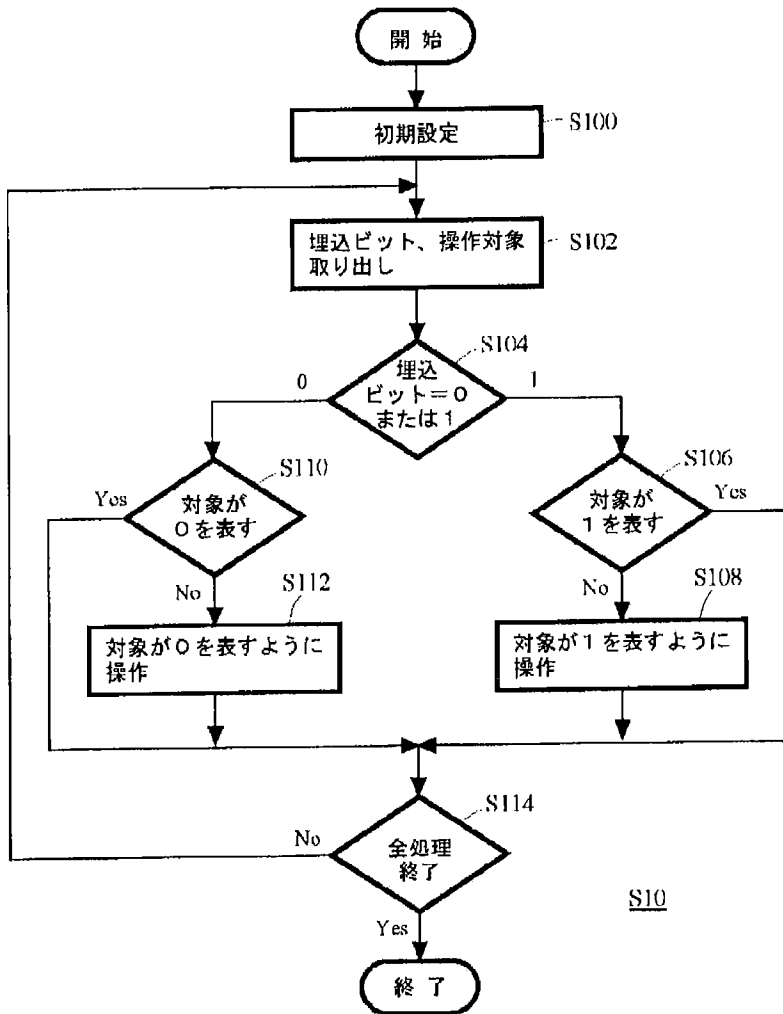
【図23】



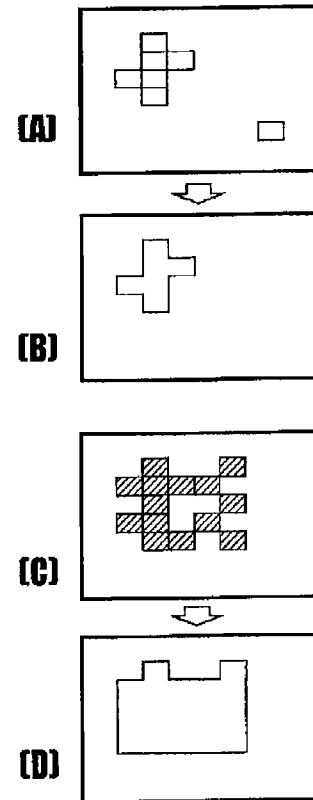
【図30】



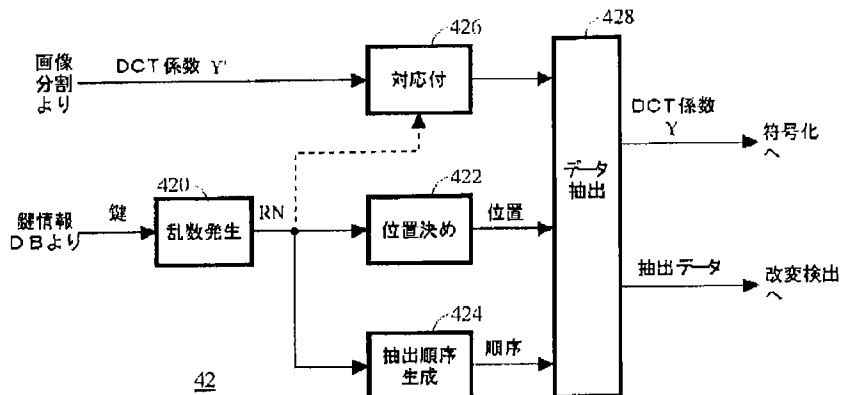
【図12】



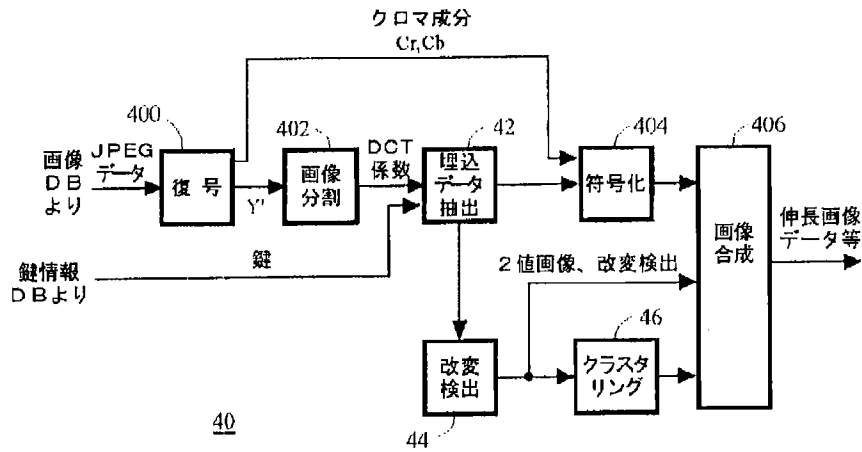
【図21】



【図14】



【図13】

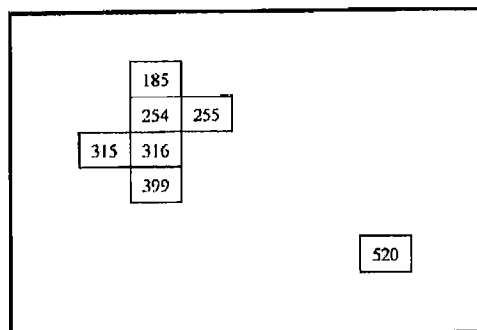


【図18】

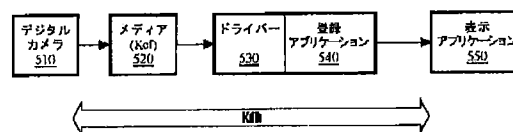
	1	2	3	4	5	96
ペア 1~96	1	0	1	1	0	1
ペア 97~192	1	0	1	1	0	1
ペア 193~288	1	0	1	1	0	1
ペア 289~384	1	0	1	1	0	1
...
ペア 6049~6144	1	0	1	1	0	1
抽出結果	1	0	1	1	0	1

64 回繰り返し (64 repetitions)

【図20】



【図28】

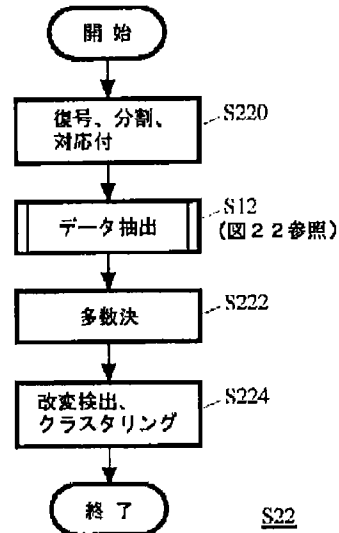


【図19】

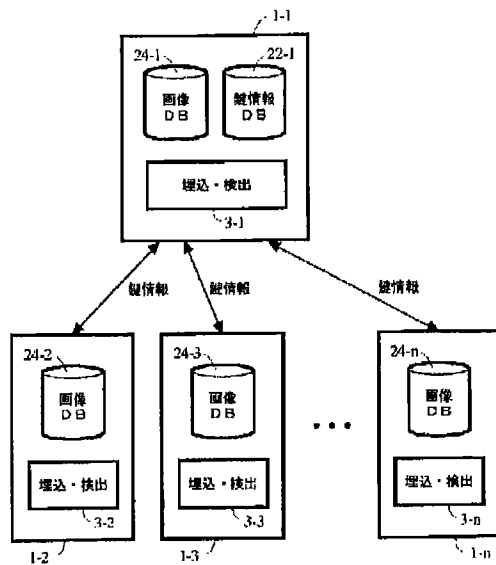
検出された埋込データのビット番号									
	1	2	3	4	5				96
ペア 1~96	ペア11 1	ペア5 0	ペア31 1	ペア9 1	0	-----			1
ペア 97~192	ペア99 1	ペア126 0	ペア150 1	ペア153 1	0	-----			ペア183 0
ペア 193~288	1	0	1	ペア255 0	0	-----			ペア254 0
ペア 289~384	1	ペア315 1	1	1	ペア316 1	-----			1
ペア 385~480	ペア399 0	0	1	1	0	-----			1
ペア 481~576	1	0	1	1	ペア520 1	-----			1
⋮	⋮	⋮	⋮	⋮	⋮				⋮
抽出結果	1	0	1	1	0	-----			1

 不整合

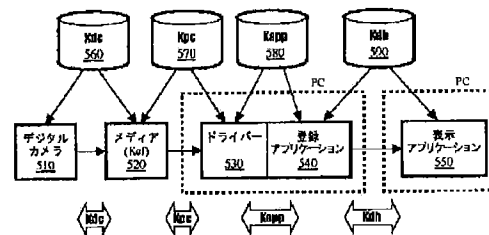
【図24】



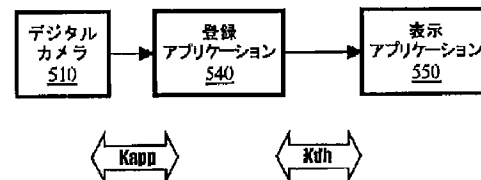
【図25】



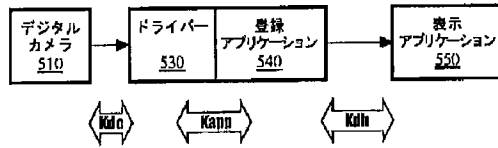
【図26】



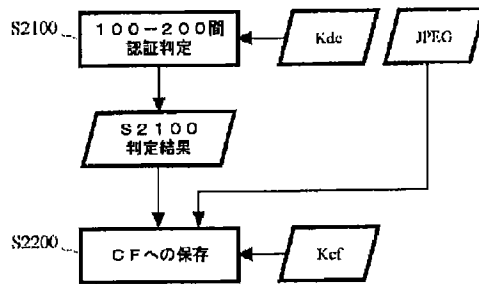
【図27】



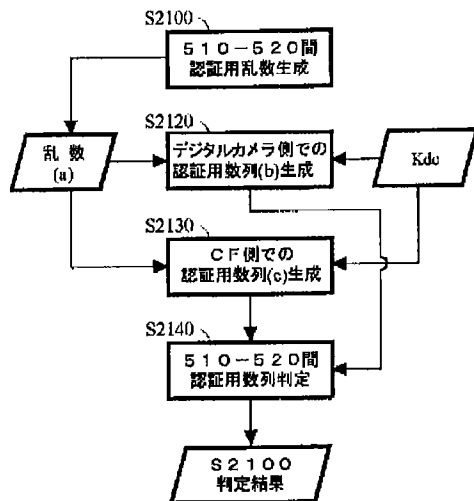
【図29】



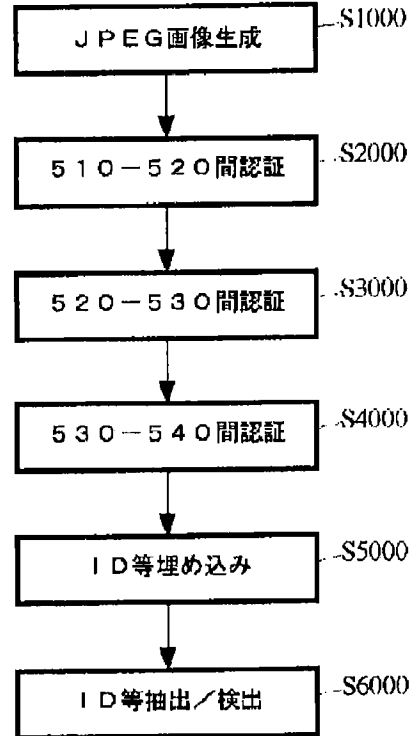
【図32】



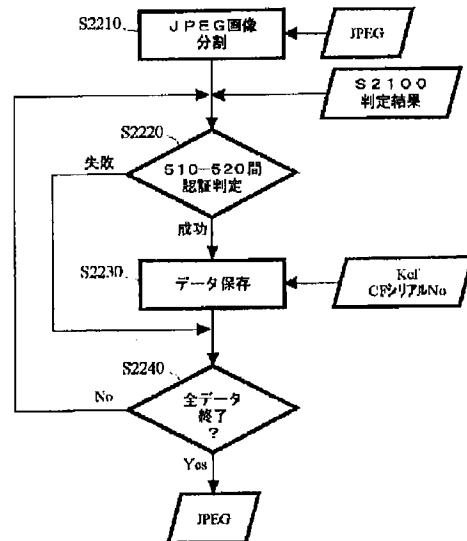
【図33】



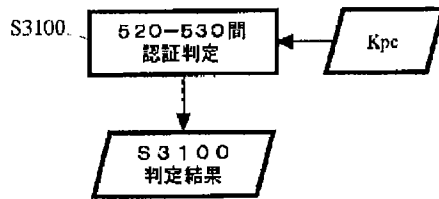
【図31】



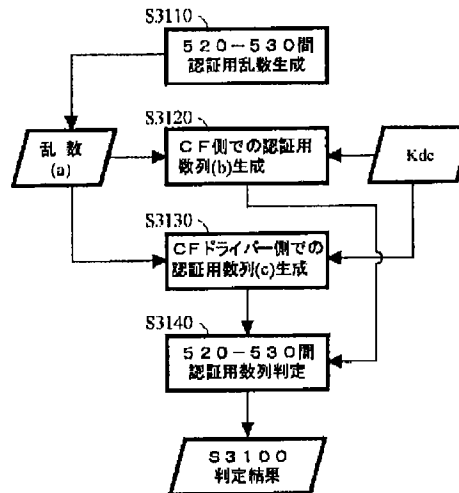
【図34】



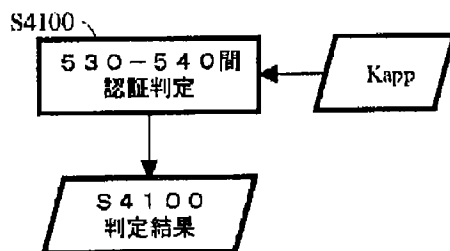
【図35】



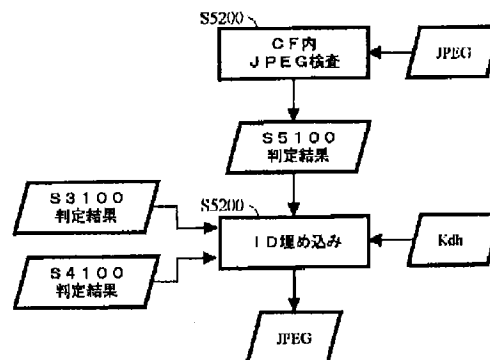
【図36】



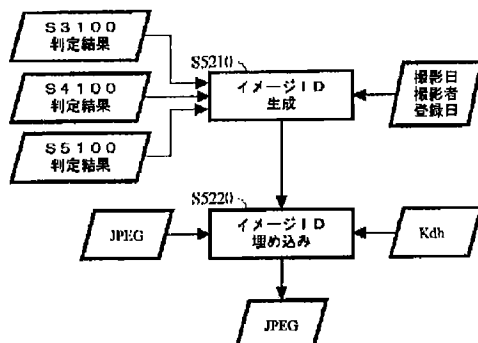
【図37】



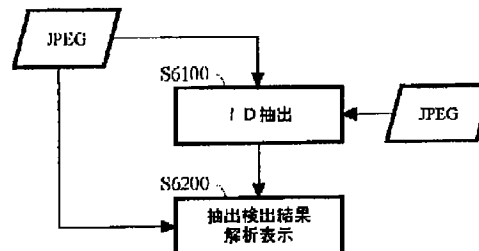
【図38】



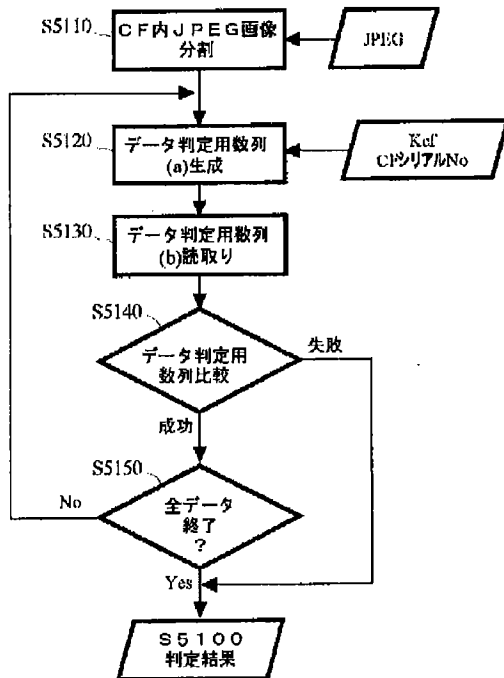
【図41】



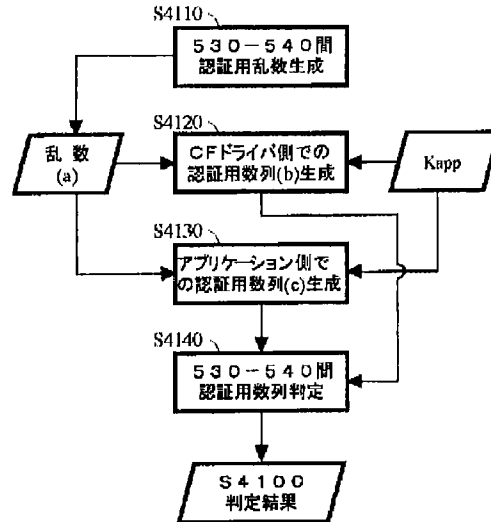
【図42】



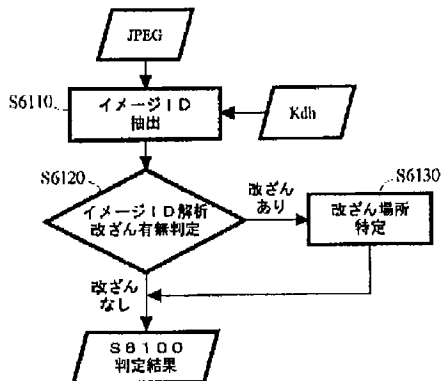
【図39】



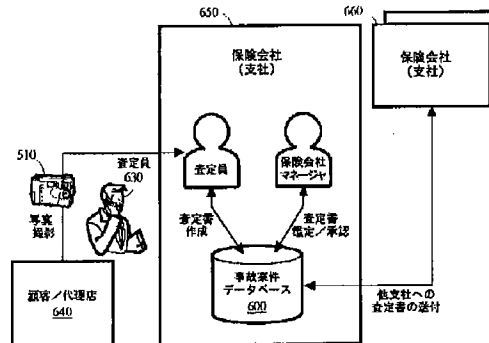
【図40】



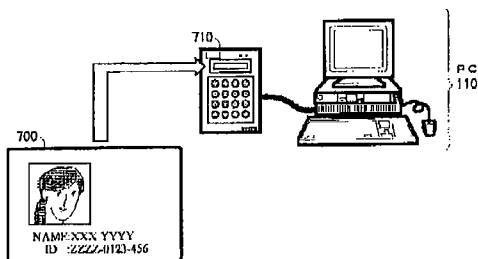
【図43】



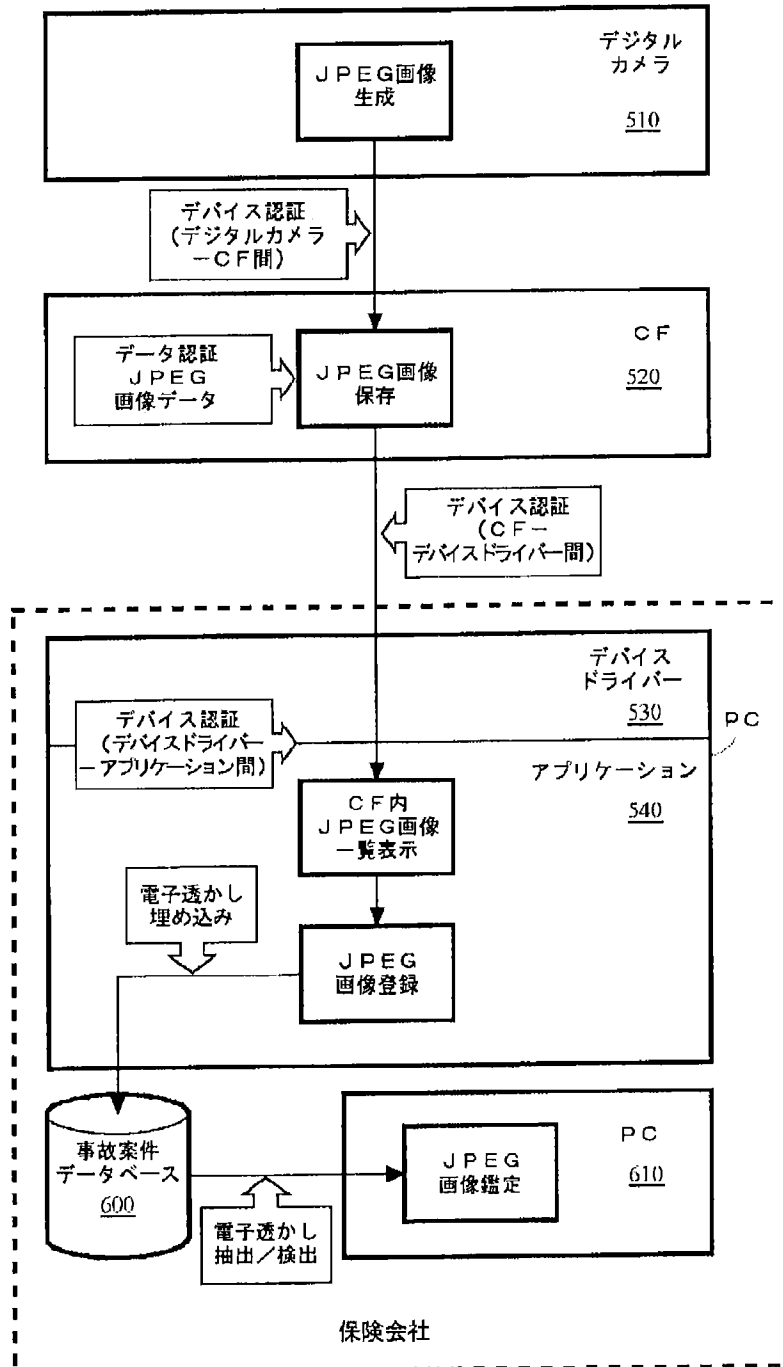
【図44】



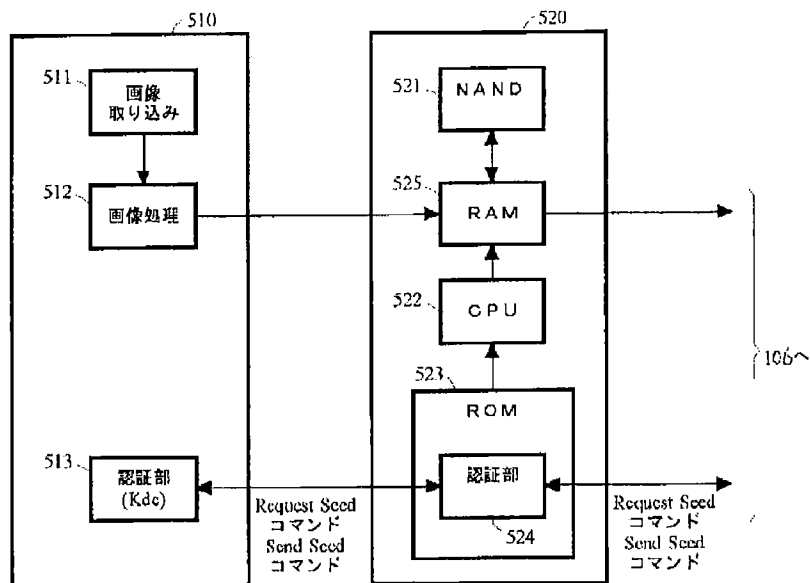
【図47】



【図45】



【図46】



フロントページの続き

(72)発明者 豊川 和治
神奈川県大和市下鶴間1623番地14 日本ア
イ・ビー・エム株式会社 東京基礎研究所
内

(72)発明者 森本 典繁
神奈川県大和市下鶴間1623番地14 日本ア
イ・ビー・エム株式会社 東京基礎研究所
内

(72)発明者 利根川 聡子
神奈川県大和市下鶴間1623番地14 日本ア
イ・ビー・エム株式会社 東京基礎研究所
内

Fターム(参考) 5C053 FA13 FA27 GB06 GB07 GB22
GB36 JA21 JA22 JA30 KA24
LA06 LA14
5C076 AA02 AA14 BA03 BA06